



NDPC
NIGERIA DATA PROTECTION COMMISSION

TRAINING GUIDE FOR DATA PROTECTION OFFICERS

This material was developed under the
AU-EU D4D Hub Project

November 2023

Table of Contents

Introduction	
Participants' Introductions and Key Expectations	07
General Information to Enhance Workshop Effectiveness	08
Section 1: Fundamental Principles of Data Protection (50min)	
Topic 1: Understanding the Fundamentals of Data Protection and Data Privacy Principles. (30min)	12
Topic 2: Determining the Balance Between Data Privacy and Fulfilling the Demands of the Business. (20min)	36
Section 2: The Crucial Role of the Data (50min)	
Topic 1: Defining the Responsibilities and Functions of Data Protection Officers (50min)	49
Section 3: Duties of Data Processors and Controllers (55min)	
Topic 1: In-depth understanding of the Roles of Data Processors and Controllers	66
Topic 2: Responsibilities of Controllers and Processors in Cases of Subcontracting or Sub-processing (30 mins)	77
Topic 3: Real-life examples of data processing scenarios (10 mins)	83



Section 4: Managing Data Security Incidents and Breaches (40min)

Topic 1:	Strategies for Identifying and Responding to Data Security Incidents (15min)	90
Topic 2:	Best Practices for Mitigating the Impact of Data Breaches and Ensuring Compliance (25min)	97



Section 5: Overview of the Nigerian Data Protection Act

Topic 1:	Legal Obligations of Data Controllers, Processors and Data Protection Officers.	109
Topic 2:	Understanding the Role of the Nigerian Data Protection Commission (NDPC)	121



Section 6: Technicalities of Data Protection

Topic 1:	Privacy Policy, Cookie Policy and Cookie Management	131
Topic 2:	Managing Third-Party Risks: Vendors, Partners and Collaborations.	142



Section 7: Information Security in Data Protection

Topic 1:	Data Encryption and Secure Data Handling Techniques	153
-----------------	---	-----



Section 8: Cross-Border Data Transfers

Topic 1:	Mechanisms of Cross-border Data Transfer	162
Topic 2:	Impact of data localization laws and data protection on global operations	169

References

List of References

- **The Nigeria Data Protection Act**
<https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf>
- **Nigeria Data Protection Act: What Individuals, Businesses and Organizations Should Know**
<https://www.banwo-ighodalo.com/grey-matter/nigeria-data-protection-act-what-individuals-businesses-and-organizations-should-know>
- **ICLG - Data Protection Laws and Regulation**
<https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria>
- <https://www.geeksforgeeks.org/what-is-data-encryption/>
- https://www.splunk.com/en_us/blog/learn/data-encryption-methods-types.html
- <https://data36.com/data-anonymization-data-masking/>
- <https://www.ibm.com/topics/encryption>
- <https://www.dot-anonymizer.com/resources/blog-en/data-masking-and-anonymization-understanding-the-different-algorithms/>
- <https://us.norton.com/content/dam/blogs/images/norton/am/types-of-encryption.png>

- https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRO00yNv6Nkxc830b-iK_cgwQg2HknOW-RGw&usqp=CAU
- <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRKMf2dIBz0CpLBYiSLMsoNWROTyVGp0DfVJg&usqp=CAU>
- <https://www.techhiveadvisory.africa/insights/operationalising-the-ndpa-bridging-digital-boundaries-with-cross-border-data-rules>
- <https://aln.africa/insight/cross-border-transfer-of-personal-data/>
- Photo by Ekaterina Bolovtsova on Pexels.com

Acronyms and Abbreviations

- **NDPA:** Nigeria Data Protection Act.
- **DPA:** Data Protection Act.
- **NDPC:** Nigeria Data Protection Commission.
- **DPIA:** Data Privacy Impact Assessment
- **ROPA:** Records of Processing Activities
- **PII:** Personally Identifiable information
- **SCCs:** Standard Contractual Clauses
- **BCR:** Binding Corporate Rules
- **SLA:** Service-Level Agreements
- **SFTP:** SSH File Transfer Protocol
- **SCP:** Secure Copy Protocol
- **DLP:** Data Leakage Prevention tool
- **TLS:** Transport Layer Security
- **SSL:** Secure Sockets Layer
- **VPN:** Virtual Private Network
- **FDE:** Full Disk Encryption
- **NDPB:** Nigerian Data Protection Bureau
- **DPIA:** Data Protection Impact Assessment
- **DPO:** Data Protection Officer
- **(SAR):** Subject Access Request

Participants Introductions and Key Expectations



To ensure the training workshop proceeds smoothly, the following activities are scheduled:

- Participant introductions
- Discussions regarding participants' expectations for the training
- Implementation of various facilitation techniques, including role plays, quizzes, case studies, group discussions, etc.
- Evaluation of participants' expectations for each training topic
- Utilization of practical assignments to gauge participants' engagement and comprehension of the training content
- Fun and informative trivia quizzes to test and improve participants' knowledge of data protection.
- Closing remarks at the conclusion of each day's training

Time Allocated: 15 mins

General Information to Enhance Workshop Effectiveness.



Free discussions



Ask questions



Participate in tasks and exercises



Avoid distractions eg. use of mobile devices

To ensure an effective training workshop, participants are required to:

- Actively engage in discussions and contribute their insights.
- Minimize distractions, including the use of mobile devices, and avoid side conversations.
- Be open to asking questions and seeking clarifications when needed.
- Demonstrate enthusiasm in participating in tasks, exercises, quizzes, and other activities.
- In case of an emergency, promptly evacuate the building following the emergency exit symbols and cooperate with fellow participants.
- Keep phones on silent mode during the training sessions.
- If it's essential to attend to a phone call, request permission from the trainer and exit the classroom to avoid disrupting the session.

All training sessions have been thoughtfully designed to equip participants with the necessary knowledge on data protection in line with the defined objectives. Your cooperation and active participation are essential to the success of this workshop

Time Allocated: 15 mins

SECTION 1

Fundamental Principles of Data Protection

Interactions and Activities



This training session is intended to accomplish the following goals:

- Participants will be introduced to the core principles of data protection, such as data minimization, purpose limitation, storage limitation, and data accuracy.
- To define the role of the Data Protection Officer (DPO) in an organisation, including the DPO's responsibilities and duties, as well as their critical role in maintaining data protection compliance.
- To identify the roles and responsibilities of data processors and controllers in data protection, when subcontracting or sub-processing data, and to provide real-life examples of data processing scenarios for practical understanding.
- To equip participants with the adequate knowledge on how to respond to data security incidents, provide guidance on developing an incident response plan, and emphasise the importance of timely and transparent communication in the event of a data breach.

Participants will benefit greatly from this training session because it will provide them with the knowledge and skills needed to:

- Ensure ethical data handling and responsible personal information management.
- Understand the critical role of a DPO in ensuring legal compliance, data security, and stakeholder trust.
- Understand the distinct roles and responsibilities of data processors and controllers in order to handle data in a secure and compliant manner.

- Manage data security incidents and breaches effectively to protect your reputation, ensure legal compliance, and maintain customer trust.

To ensure a smooth facilitation of Data Protection Officer (DPO) training workshop, we shall briefly discuss the following:

- Your expectations for the training.
- Your previous knowledge on data protection to tailor our discussions accordingly.
- A discussion on data breaches that some of us may be familiar with.
- Goal sharing from selected participants.
- Engaging trivia quizzes to test and enhance your data protection knowledge.

As we progress further into the training, we will gain a comprehensive understanding of the roles, responsibilities, and obligations of a Data Protection Officer (DPO).

Topic 1

Understanding the Fundamentals of Data Protection and Data Privacy Principles including its principles.

Under this topic, the following key areas shall be discussed:

- 1.1.1 Learning Expectations
- 1.1.2 Importance of Data Protection and Data
- 1.1.3 Defining Data Protection and Data Privacy
- 1.1.4 Key Principles of the Nigeria Data Protection Act

Within this section, we will explore the Nigeria Data Protection Act of 2023, dissecting its fundamental goals, essential provisions, and the substantial consequences it carries for data protection procedures in Nigeria.

Time Allocated: 20 mins



Understanding the Fundamentals of Data Protection and Data Privacy Principles including its principles.

1.1.1 Learning Objectives

Upon completion of Topic 1 “Data Protection Fundamentals”, participants shall be equipped with the skills to:

- Understand the core of Data Protection and Privacy Principles
- Understand how to balance Data Privacy with Business Requirements
- Understand and apply the fundamental data protection principle.

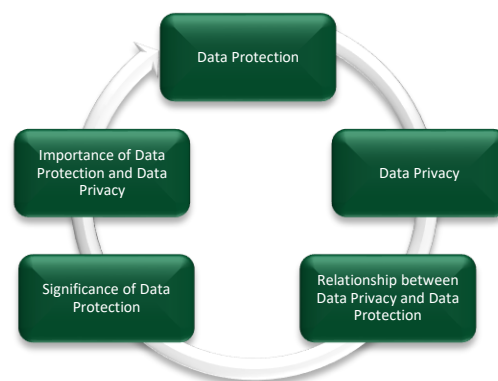




Understanding the Fundamentals of Data Protection and Data Privacy Principles.

Introduction to Data Protection and Data Privacy

"Data privacy and protection are paramount in both digital and physical realms, encompassing the practise of keeping private information about individuals safe from unauthorised access or disclosure. They establish the foundation for trust, regulation, and the protection of people's fundamental privacy rights.



What you need to know about data protection and data privacy!

Data protection and privacy are the most important things in today's constantly changing digital world. Data security is more than just the law; it is the moral and legal foundation on which modern companies build their data management practises. It takes a whole-person method to make sure that all kinds of personal data are handled with the utmost care, responsibility, and openness. Data security is not just about following the law; it's what trust, honesty, and following the law mean in the world of data management.

Data security is based on the idea that personal information should be handled safely and appropriately. It shows how important it is for businesses to protect people's privacy and rights by gathering, utilizing and storing data in a way that respects privacy and autonomy.

Currently, when information moves faster than ever, keeping personal information safe has become very important. Data Privacy and Data Protection are two basic ideas that are very important in this case. Making sure the purity and safety of personal information is based on these ideas.

- Data Protection
- Data Privacy

Before we talk about what they mean, let us talk about why they are so important in this modern age.



1.1.2 Importance of Data Privacy and Data Protection:

- **Protecting Personally Identifiable Information (PII):** Data privacy is crucial because it provides the framework for safeguarding PII such as:- a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of an individual; sex life political opinion, race, etc (see definition of personal data and sensitive personal data under Section 65 of the NDPA).
- **Preserving Trust:** Maintaining data privacy is essential for building and preserving trust with customers, clients, and users. When individuals trust that their data will be handled responsibly, they are more likely to engage with organizations.
- **Legal Compliance:** Many countries and regions have stringent data protection regulations. Failing to comply with these regulations can result in legal repercussions, including fines and sanctions.
- **Ethical Considerations:** Respecting data privacy is not just a legal obligation but also an ethical one. Treating personal data with respect and responsibility is a fundamental ethical practice in the digital age.
- **Global Data Sharing:** In an interconnected world, data is often shared across borders. Effective data protection laws facilitate international data transfers, ensuring Nigerian organizations meet the required standards for cross-border data exchange.
- **Prevention of Fraud:** Effective data protection measures help prevent fraud and unauthorized access
- **International Relations:** Complying with data protection standards can aid Nigeria's standing in the global community and facilitate cooperation with other countries.



1.1.3. Definition of the Data Privacy and Data Protection!

Data Protection: on the other hand, data protection is the practical implementation of the policies and procedures established for data privacy. It involves the use of secure tools, technical measures, and controls to ensure that data is kept safe and secure. This includes encryption, access controls, authentication mechanisms, firewalls, data backups, and other security measures designed to enforce the policies and protect data from unauthorized access or breaches.

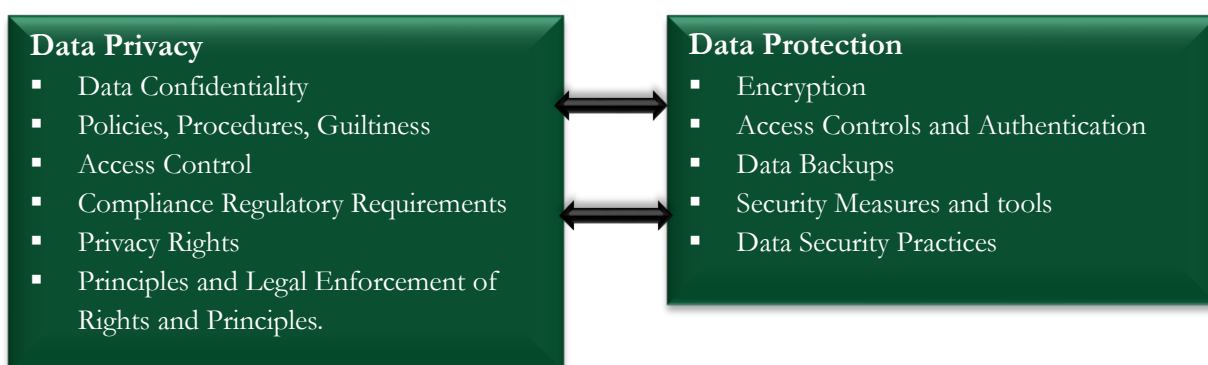
Data protection is like having security guards for your personal information. They use special tools to keep your data safe, like strong locks on your doors. They make sure your info is kept hidden from people who shouldn't see it, and they guard it against bad things happening, just like protecting your favourite assets from getting lost or broken. Data protection follows the rules of data privacy to keep your data secured.

Data Privacy: Data privacy is primarily concerned with defining and establishing policies and procedures that govern how data should be handled, who has access to it, and the rules that dictate its usage. It's about setting up the framework to protect the confidentiality, integrity, and availability of data. Data privacy often involves legal and regulatory compliance, as well as defining user roles and access permissions.

Data privacy means you have the right to control your personal information. It's like having a lock on your diary, and you get to decide who can read it and why. Your secrets are kept safe, and no one can process your information except in the manner recognized by law.

It is also important that we understand Data Security is a broader concept that includes protecting not only personal data but all forms of data within an organization. It involves the implementation of measures and protocols to defend data from unauthorized access, data breaches, and other threats. Data security covers areas such as network security, application security, and physical security to maintain the confidentiality, integrity, and availability of data.

The relationship between data protection and data privacy.



The relationship between data protection and data privacy is one of interdependence.

while Data privacy, on the other hand, revolves around individuals' rights and preferences regarding the collection and use of their personal information, often guided by legal regulations

Data protection focuses on securing data from unauthorized access and breaches, employing security measures like encryption and access controls



Nigeria Data Protection Act 2023 is designed to:

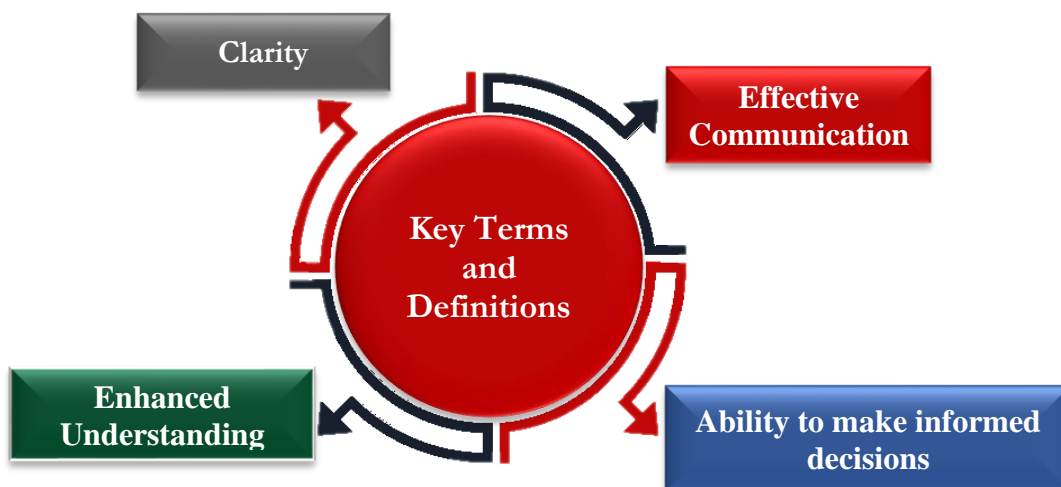
- Protect the rights of data subjects by ensuring that personal data is processed in a fair, lawful and accountable manner.
- Promote data processing practices in Nigeria that guarantee the security of personal data and ensure the privacy of data subjects.
- Provide the legal framework for regulating and safeguarding personal data, and the means of recourse and remedies where the rights of data subjects have been breached.
- Ensure that data controllers and data processors fulfil their obligations to data subjects.
- Safeguard data subjects' fundamental and constitutional rights, freedom and interests, and establish an impartial, independent and effective regulatory body to supervise data controllers and data processors and superintend over data protection and privacy issues; and
- strengthen the legal foundations of the national digital economy and guarantee the participation of Nigeria in the regional and global economies through beneficial and trusted use of personal data.



Understanding the Fundamentals of Data Protection and Data Privacy Principles.

Overview of Data Protection and Data Privacy Key Terms

It is significantly important to fully understand the important terms and meanings used in the field of Data Protection, mainly because of the important reasons listed below:



Data Protection Officers (DPOs) must have a full understanding of all the important terms and definitions used in data protection." These terms lay the groundwork for their important job of protecting data privacy and following the rules. DPOs can effectively manage the complex landscape of data protection and carry out their duties in protecting individuals' personal data by becoming familiar with these definitions



Data Protection key terms and definitions are outlined below:

- **Personally Identifiable Information, or PII**, is any data that can be used to identify a person or find out who someone is. This includes names, addresses, phone numbers, email addresses, Social Security numbers, and biological data. It is very important to protect PII for data security.
- **Data Controller:** The controller is the entity responsible for determining the purpose and means of processing personal data. They are the decision-makers when it comes to how and why data is processed.

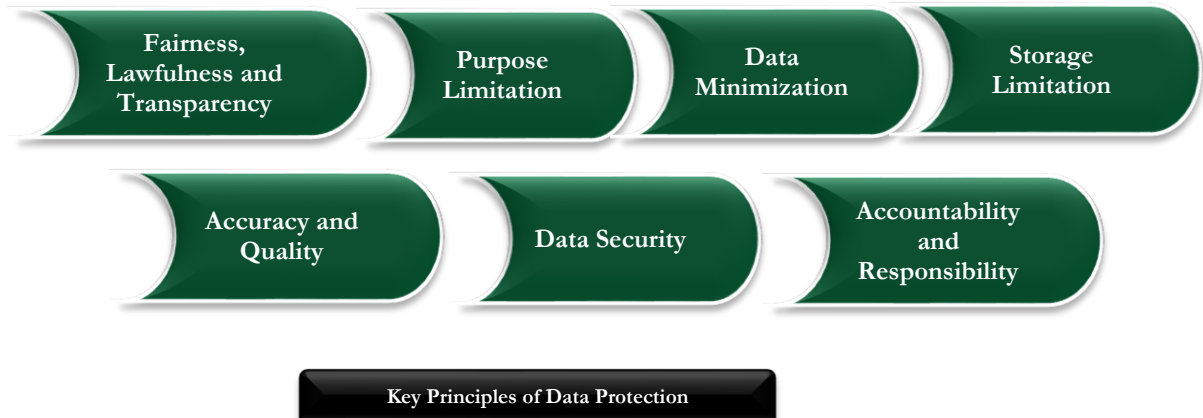
- **Data Controller or Processor of Major Importance:** This term applies to organizations that manage a substantial volume or have significant value associated with the personal data they handle. They often have more extensive responsibilities and obligations under data protection regulations.
- **Data Processor:** A processor is an entity that processes personal data on behalf of a data controller. They carry out data processing activities according to the instructions of the controller.
- **Data Subject:** The data subject is the individual to whom the personal data pertains. In the context of data protection, the data subject has rights regarding the use of their data and how it's handled.
- **Sensitive Personal Data:** This category includes particularly sensitive information, such as genetic, biometric, racial, health-related, or other details that may require enhanced protection due to their nature.
- **Data Breach:** A data breach occurs when there is unauthorized access to or loss of personal data. Such incidents can result in the exposure of individuals' sensitive information, potentially leading to privacy and security concerns.
- **Pseudonymisation:** Pseudonymisation is a method of processing data in such a way that it cannot be directly linked to an individual without additional information. It enhances data privacy and security.
- **Data Portability:** Data portability allows individuals to transfer their personal data between different systems or organizations, providing them with more control over their information.
- **Records of Processing Activities (ROPA):** ROPA is a document that lists an organization's data processing activities. It serves to promote transparency and compliance, allowing individuals and authorities to understand how data is being handled.
- **Consent:** Consent involves obtaining voluntary permission from an individual for the use of their personal data. It is a fundamental element of data protection and privacy, emphasizing the importance of an individual's agreement in data processing.
- **Data Minimization:** Data minimization involves the practice of collecting only the data that is strictly necessary to achieve a particular purpose. It is an essential step in reducing privacy risks.



Understanding the Fundamentals of Data Protection and Data Privacy Principles.

1.1.4 Key Principles of Data Protection

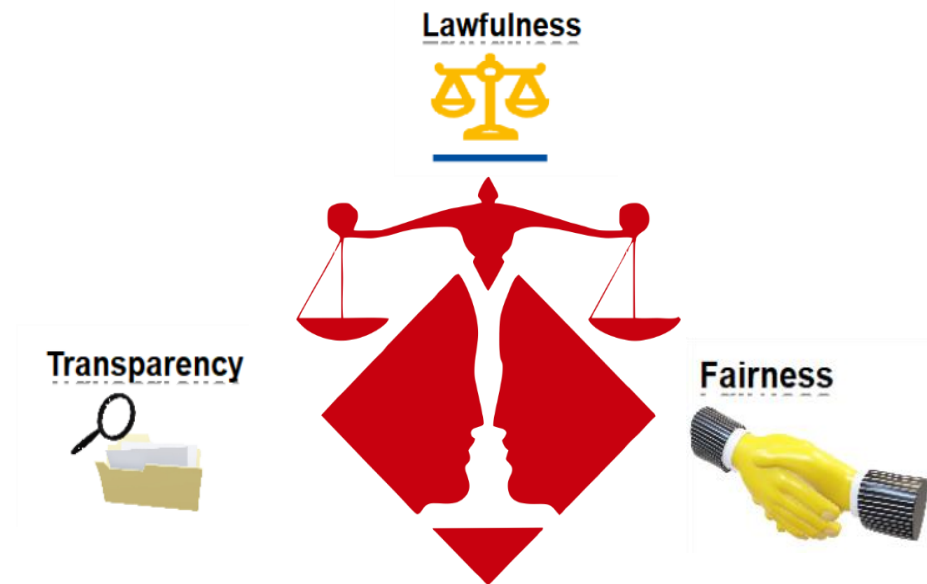
The Key Principles of Data Protection that all Data Protection Officer must adhere to include



Data protection principles are the fundamental values underlying ethical and secure data management practises. These principles, as outlined in the Nigeria Data Protection Act, 2023, lay the groundwork for the responsible and transparent management of personal data. They incorporate legality, fairness, and transparency in data processing, ensuring that the privacy and rights of individuals are respected at every stage of data handling.

Understanding the Fundamentals of Data Protection and Data Privacy Principles.

Fairness, Lawfulness and Transparency



The Fairness, Lawfulness, and Transparency Principle

One of the fundamental pillars of data protection is the principle of fairness, lawfulness, and transparency. It embodies the concept that organizations must process personal data in a manner that is fair to the individuals whose data is being collected and processed, within the bounds of the law, and with complete transparency.

The principles of fairness, lawfulness, transparency, are essential foundations of data protection. Your job as a Data Protection Officer (DPO) is essential to making sure that this principle is followed by your company. Let's explore it in detail using examples to highlight each feature:

Fairness: Fairness in data protection means respecting individuals' rights, preventing harm, obtaining informed consent, and minimizing data collection to ensure equitable and ethical data handling.

Fairness means treating individuals, whose data is being processed, with respect and equity. It involves ensuring that data processing does not harm or put individuals at a disadvantage. For example, it's fair to collect customer data for order processing but not to use it for unrelated

purposes like targeted advertising without consent and as a DPO to make sure that data processing does not unfairly hurt or disadvantage people. If your company gathers consumer information, for instance, for marketing purposes, you should make sure that the data is utilised for marketing-related endeavours and not for unrelated objectives, such as loan decisions. The fairness principle is upheld in this.

Lawfulness: Lawfulness entails having a valid legal basis for data processing, adhering to relevant data protection laws, and implementing data security measures to protect against unauthorized access or damage.

Lawfulness emphasizes that data processing must always adhere to applicable laws and regulations. As a Data Protection Officer (DPO), your role involves ensuring that your organization's data processing activities are compliant with the existing legal and regulatory law. For instance, processing employee data for payroll must comply with labour laws and tax regulations.

Transparency: Transparency is about being open and clear in all data-related activities. It involves providing individuals with information about how their data is collected, used, and shared. Transparency ensures that individuals are well-informed and can make decisions about their data with full awareness. It includes clear and concise privacy policies, informed consent processes, and making data subject rights easily accessible.

In simple terms transparency requires providing individuals with clear, understandable information about how their data is collected, used, and shared. As a DPO, you play a pivotal role in maintaining open communication. For example, a transparent privacy policy should clearly state the purposes of data collection, helping individuals make informed decisions about their data.

People must be informed about the collection, usage, and sharing of their data in order for there to be transparency another example of this might be, "We collect your email address to send you our newsletter." Transparency like this helps people make decisions regarding their data that are well-informed.



Importance for Lawfulness, Fairness, and Transparency Principles:

- Compliance with this principle promotes trust between organizations and individuals by assuring them that their data will be handled fairly and in accordance with the law.
- Organizations reduce the risk of legal consequences, penalties, and sanctions that may result from data protection violations by adhering to the law.
- Transparency in data processing practices reflects favourably on a company's reputation and demonstrates ethical conduct.
- Conformity to the Nigeria Data Protection Act, 2023 which is a lawful mandate.



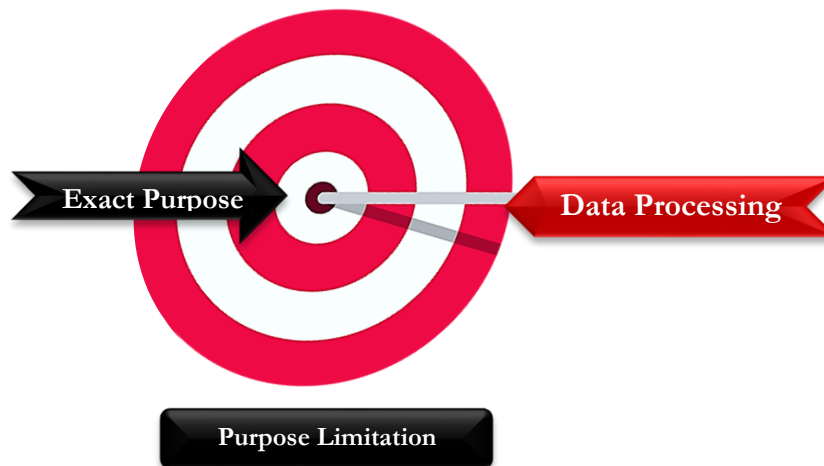
These considerations are crucial for a Data Protection Officer (DPO) to ensure adherence to the Lawfulness, Fairness, and Transparency Principles:

- To maintain transparency and justice in data management, clearly disclose to Data Subjects the reasons for data processing.
- Before collecting and processing personal data from individuals, obtain explicit and informed consent from them, emphasising the importance of fairness and legality.
- Ensure that all data collecting and processing activities strictly correspond to legal and regulatory norms, with the principle of lawfulness as the primary focus.
- Keep complete records of all data processing activities in order to demonstrate openness and transparency to both data subjects and regulatory authorities.
- Create data protection policies and procedures that are transparent, in accordance with legal frameworks, and accessible to employees and key stakeholders, fostering fairness and transparency.
- Conduct regular audits and evaluations of data processing practises to identify and rectify any potential compliance issues, guaranteeing continued adherence to legality, fairness, and transparency principles.

Understanding the Fundamentals of Data Protection and Data Privacy Principles.

Purpose Limitation

Purpose limitation in data protection limits the collection and processing of personal data to defined legal purposes. This promotes clarity and understanding of processing purposes by Data Subjects



The Purpose Limitation Principle

The principle of purpose limitation in data protection mandates that organizations must clearly define and express the specific objectives for which they acquire and process personal data. This concept guarantees that data is only utilized for lawful and clearly specified purposes, hence prohibiting any subsequent processing that is inconsistent with the original intentions.

The Importance of Purpose Limitation Principle

One important data protection principle is the Principle of Purpose Limitation, which highlights the necessity for organisations to explicitly define and restrict the objectives for which they gather and use personal information. This principle makes sure that any future uses of personal data are consistent with the original purposes for which it was gathered. To preserve people's right to privacy and abide by data protection laws, organisations must minimise data collecting, be open and honest about their data processing operations, and get informed consent where needed. This idea supports the upkeep of transparency, trust, and moral data management procedures.

- Organisations that clearly explain why they collect and manage personal information are trusted by data subjects. Businesses need trust to build ethical relationships with customers. People are more likely to give their personal information for legitimate reasons.
- Purpose restriction enhances transparency. Data subjects have a right to know how their data is used. Openly declaring these goals shows data processing transparency. An organization's credibility improves with transparency.
- Personal data misuse is prevented by setting clear objectives. This reduces the likelihood of companies collecting data for unrelated purposes. Selling or using data without permission can damage an organization's reputation and legal standing.
- Organisations reduce risks by limiting their purpose. They only process data when necessary and for specific reasons, reducing the risk of unintentional or illegal data breaches.
- Purpose limitation helps Data Subjects make informed decisions about sharing personal information. Users can consent when they understand why their data is collected and used. Respect for autonomy promotes privacy.



The seven major tasks and considerations for a Data Protection Officer (DPO) in ensuring adherence to the Principle of Purpose Limitation are as follows:

- Collaborate with the organisation to clearly define and document the exact purposes for collecting and processing personal data, ensuring compliance with the lawful basis for processing.
- Conduct regular audits and analyses of data processing operations to ensure that they are aligned with the specified purposes and that compliance is maintained
- Carefully document any changes in data processing purposes and guarantee transparent and timely contact with data subjects.
- Encourage data minimization practices across the organization. Instruct staff to collect and process only the data that is necessary for the defined purposes, avoiding over-collection
- Maintain complete records of data processing operations, including purposes, data, and the legal basis, as well as easily available records of data subject permission acquired.



Understanding the Fundamentals of Data Protection and Data Privacy Principles.

Data Minimization

The data minimization principle in data protection emphasizes collecting only the necessary personal data, reducing privacy risks, and ensuring compliance.



Data Overload



Efficient Data Minimization



The Data Minimization Principles

Data minimization means that a company should be careful about what personal information it gathers and how it uses it. It says that personal information should only be used for the reason it was gathered, and that extra or unnecessary information should be avoided.

If a company needs to handle customer data to fulfil an order, for example, it should only get the customer's name, shipping address, and payment information. It would be pointless and might even be harmful to the customer's privacy to ask for extra information, like their favourite colour or hobbies.



Importance of data Minimization Principles

- Organizations reduce risk of data breaches, unauthorized access, and privacy violations by restricting personal data collection and storage. Data minimization reduces security risks.
- The Nigeria Data Protection Act, 2023 and other data protection regulations such as the GDPR compel organizations to minimize data.
- Respecting privacy is essential. Data minimization shows an organization's dedication to data security and privacy.



Data Protection Officer (DPOs) should take numerous actions to comply with data minimization principle through the following:

As a Data Protection Officer (DPO), one of your duties is to make sure that personal data is only collected and used for the reasons it was collected in the first place. You should also encourage others to do the same. These are the main ideas:

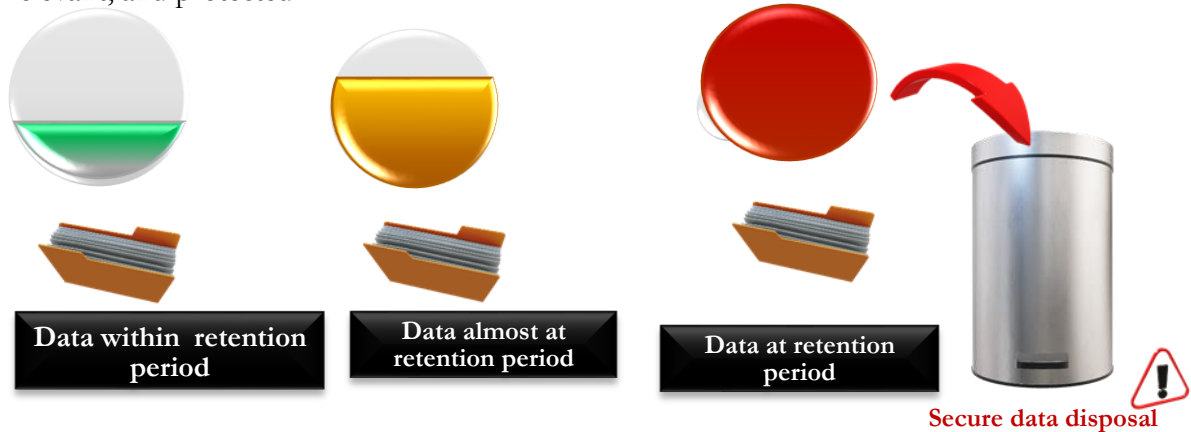
- Make sure that personal information is only gathered for clear, defined, and acceptable uses. DPOs must assess and approve these reasons in order to avoid excessive data acquisition.
- Keep track of all personal information and how it is used inside the company, eliminating any information that is superfluous or redundant.
- Establish and implement explicit data minimization guidelines for staff members that cover data gathering, processing, and storage. All pertinent parties should be informed about these policies.
- To help staff members understand the value of data minimization and their part in upholding it, offer them thorough training and awareness programmes.
- Make data audits a regular practise by conducting regular data audits and evaluations to find and rectify instances of non-compliance with data minimization.
- Promote data reduction techniques and stress the importance of reducing data gathering and processing by working with management at all levels.
- To assist with data reduction initiatives, set aside funds for infrastructure, technology, and training in data protection.
- Make sure that data minimization procedures and corporate policies are applied consistently, and take appropriate action when non-compliance occurs.
- To prioritise data safety across the entire organisation, incorporate data minimization from the beginning into processes, systems, and initiatives.



Understanding the Fundamentals of Data Protection and Data Privacy Principles.

Storage Limitation

Storage limitation, a fundamental data protection principle, dictates that personal data should not be stored longer than necessary for its intended purposes, ensuring data remains accurate, relevant, and protected.



The Storage Limitation principle

A key idea in data protection is the principle of storage limitation, which states that companies should only retain personal information for as long as it is required for the purposes for which it was gathered. The concept of storage limitation involves the following:

- **Respect for Privacy:** It's like acknowledging that people's personal data is their own, and you shouldn't hang onto it indefinitely. Keeping data longer than needed can be invasive and pose privacy risks.
- **Data Accuracy:** Data can get outdated, like old newspapers. By not storing it forever, you ensure that the data you have is more likely to be accurate and reliable.
- **Security:** The longer you keep data, the more you need to protect it. By limiting storage, you reduce the amount of data you have to safeguard, which enhances security.
- **Legal Compliance:** Many laws require organizations to only keep data for as long as it serves its original purpose.
- **Efficiency:** Hanging onto unnecessary data is like hoarding—it's not efficient. By limiting storage, you streamline your operations, saving resources and making it easier to respond to data access requests or breaches.



Importance of Storage Limitation principle

Storage limitation is important for many reasons:

- It ensures that organizations don't hold personal data longer than necessary. This decreases data breach risk.
- Storing data for too long might lead to obsolete or erroneous information, which can harm decision-making and data quality
- Storage limitation principle is mandated by several data protection laws, including the Nigeria Data Protection Act, 2023 and other data protection laws globally. Breaking these restrictions might result in severe fines and legal issues.
- Storage limitation practices show a commitment to privacy and rights. Data transparency is further promoted.



The role of the Data Protection Officer (DPO) in ensuring adherence to the principle of storage limitation involves various crucial responsibilities and actions:

- Work with the organisation to compile a thorough inventory of all personal data held, including its sources and objectives.
- Collaborate with the organisation to create and record specific data retention rules. These policies should establish the periods for retaining various types of data and must be consistent with the original goals for which the data was gathered.
- Implement data deletion methods that are both secure and permanent. When data reaches the end of its defined retention period or is no longer required for its intended purpose, these procedures should be activated.
- Conduct periodical data audits to determine the relevancy of stored data. Any data that has outlived its retention period or is no longer required for its intended purpose should be identified and deleted.
- Ensure that the organization's consent management mechanisms allow individuals to easily withdraw their consent.
- Encourage and facilitate management's active participation in designing and implementing data retention rules. These policies should be consistent with the organization's data processing activities and should be evaluated for compliance on a regular basis.



Understanding the Fundamentals of Data Protection and Data Privacy Principles including its principles.

Accuracy and Quality

Accuracy and quality, as a data protection principle, emphasize the importance of maintaining precise, up-to-date, and error-free personal data to ensure its reliability and integrity.



Accurate Data



Enhanced Data Quality



Enhanced Data Protection



The Accuracy and Quality Principles

The Accuracy and Quality principle, in the context of data protection and privacy, is a fundamental guideline that emphasizes the need to maintain accurate, up-to-date, and high-quality personal data. This principle underscores the following key points:

Accuracy Data: Personal information should be correct and free of mistakes. It is up to organisations and DPO to make sure that the information they gather and store is correct. Data that isn't correct can cause confusion, bad decisions, and even harm to individuals.

Data Quality: The collected data should be relevant, appropriate, and useful for the purpose it was collected for. It stops people from gathering too much or useless information. The quality of the data should be good enough to do what it was collected to do.



Importance of Accuracy and Quality Principles

- Accurate and high-quality data enables organizations to make educated and accurate decisions, hence minimizing the likelihood of errors in important processes.
- Ensuring the precision of data cultivates trust among individuals and entities involved, thereby bolstering the organization's standing as a responsible steward of data.

- Numerous data protection regulations, such as the Nigeria Data Protection Act (NDPA) and General Data Protection Regulation (GDPR), mandate that organizations guarantee the precision of personal data. Failure to comply can result in legal repercussions.



The role of the DPO in ensuring adherence to this principle

- A Data Protection Officer (DPO) is responsible for making sure that the Accuracy and Quality principle is followed. This is done by overseeing and putting in place steps to keep personal data accurate and of high quality. Here are the main things that a DPO needs to do in this case:
 - During the data collection process, the DPO should push for and set up validation protocols. This includes putting in place checks and procedures to make sure that mistakes are kept to a minimum when entering data, so that correct and trustworthy data is gathered from the start.
 - Any mistakes or inconsistencies in stored data should be found and fixed regularly through regular data audits. The DPO should oversee these audits to make sure they work.
 - The DPO should work with the right departments to create and write down protocols for updating data correctly and on time. This is very important for keeping data up to date and useful.
 - DPO should oversee making and following rules and instructions that put data quality and accuracy first. The DPO should make sure that these rules are in line with the law and the organization's goals.
 - Tell Data Subjects about any mistakes in their information and ask that it be fixed. The Data Protection Officer (DPO) should make sure that people can easily and clearly voice concerns about data quality.
 - The DPO should set up thorough training sessions for the people who are in charge of entering and maintaining data. It should be emphasised in this training how important accurate data is and what each staff member can do to keep it that way.
 - The DPO should keep an eye on how data quality policies are being followed and make changes as needed to make sure they are being followed. This includes quickly looking into and fixing problems with the quality of the data



Understanding the Fundamentals of Data Protection and Data Privacy Principles.

Data Security

Data security is not only important but also an essential component of data protection, as there can be no effective protection without security.



Data security refers to the practice of protecting digital information from unauthorized access, corruption, or theft throughout its lifecycle. It encompasses a wide range of measures and practices designed to ensure the confidentiality, integrity, and availability of data.

Data security is a fundamental principle of data protection, encompassing the safeguarding of personal data against unauthorized access, intrusions, and loss. It is essential to implement security measures to enhance protection of personal data.

- **Confidentiality:** Ensuring that personal information is accessible only to authorised users and is protected against unauthorised access or disclosure.
- **Integrity:** Maintaining the accuracy and dependability of personal data while preventing unauthorised alterations, corruption, or tampering.
- **Authentication and Authorization** entails confirming the identity of individuals and systems with data access and defining the actions they are permitted to perform.
- **Encryption:** The use of encryption to safeguard data during storage and transmission by rendering it unreadable to unauthorised parties.
- **Access controls** to define who can access data and what actions they can perform, including user permissions, role-based access, and the principle of least privilege.

Importance of Data Security Principle

- Data security ensures the confidentiality of personal data, promoting trust among Data Subjects and stakeholders who anticipate that their information will be kept secret.
- Numerous data protection regulations mandate the implementation of stringent data security measures. Noncompliance can result in severe sanctions.
- Effective data security measures protect personal data against intrusions, thereby reducing the likelihood of data loss, unauthorized access, and identity theft.
- Organizations with a strong commitment to data security develop a reputation for responsible data management, which provides them with a competitive advantage.

What the DPO know about the Data Security Principle

For organizations to maintain conformance with the data security principle, the following practices can be implemented:

- Employ access control measures to restrict data access to authorized personnel only, assuring the confidentiality and security of data.
- Encrypt sensitive data during transmission and storage to prevent unauthorized access and preserve data secrecy.
- Conduct periodic security audits and vulnerability assessments to identify and address potential security vulnerabilities.
- Develop and implement a plan for responding to data breaches in a prompt and effective manner.
- The management shall direct the creation and implementation of data security policies and procedures that comply with applicable data protection regulations.
- Provision of oversight for data security practices, monitor compliance, and respond to security incidents with corrective action.
- Develop and implement a plan for responding to and mitigating the impact of security incidents



Understanding the Fundamentals of Data Protection and Data Privacy Principles.

Accountability and Responsibility

Assure organisational responsibility for data protection guidelines, put compliance demonstration plans into action, and promote openness in data processing.



Accountable



Responsible



The Nigeria Data Protection Act, 2023 outlines several fundamental rights that individuals have concerning the processing of their personal data. These rights are essential for maintaining the privacy and security of individuals' information in the digital age. They provide individuals with significant control over how their data is collected, used, and managed. Let's explore these key rights in more detail.



The Accountability and Responsibility-principle.

The "Accountability and Responsibility" principle in the Nigeria Data Protection Act, 2023 says that companies that gather and use personal data must make sure they follow the rules for data protection. This principle stresses that businesses should be serious about their data protection duties and be able to show that they care about data privacy and security and it is expected that the following are adhered to

- Organisations bear accountability for the personal information they gather and handle. This implies that they have to abide by the legal requirements and data protection principles set forth in the NDPA.
- All NDPA requirements, such as securing authorization for data processing, guaranteeing data accuracy, capping data storage, and upholding data security, must be complied with by organisations.

- Businesses must maintain records of all of their data processing operations, policies, and procedures related to data protection. It is crucial to have this documentation in order to prove compliance.
- Establishing procedures to hold organisations accountable for data protection is a good idea. This entails designating a Data Protection Officer (DPO) and establishing explicit procedures for managing requests from data subjects and data breaches.



Importance for Accountability and Responsibility

- Making sure that data protection laws and regulations are followed in order to stay out of trouble with the law and avoid penalties.
- Gaining the trust of data subjects requires handling data responsibly and upholding their rights.
- Improving data security to reduce the possibility of illegal access and data breaches.
- Reputation protection is the process of preserving the brand and reputation of the company by showcasing a dedication to moral and responsible data processing.



What the DPO know about the Accountability and Responsibility Principle

- The DPO oversees managing an organization's data protection practises and ensuring that data protection rules are followed.
- The DPO should be aware of all personal data processed by the organisation. This involves understanding what data is gathered, how it is utilised, and where it is kept.
- DPIAs are an essential component in demonstrating accountability. The DPO should oversee the process of performing DPIAs to identify and mitigate privacy concerns associated with data processing operations.
- The DPO should make certain that the organisation has detailed records of its data processing operations, rules, and processes.
- The DPO should collaborate with the organisation to create and implement data security policies and procedures. These documents should detail how personal data is processed as well as how data subjects' rights are protected.

Topic 2

Determining the Balance Between Data Privacy and Fulfilling the Demands of the Business

Under this topic, the following key areas shall be discussed:

- 1.2.1 Learning Objectives
- 1.2.2 Balancing Data Privacy and Business Operations
- 1.2.3 Comprehensive Strategies for Data Protection and
- 1.2.4 Challenges Faced by Businesses in Data Privacy and their consequences.
- 1.2.5. Interactive discussions

As a Data Protection Officer (DPO), one of your primary roles is to understand how to balance the need for privacy with the need for business. During this training, the main goal will be to give DPOs the information and skills they need to effectively navigate this complicated area.

This lesson covers the most important parts of following data protection rules, with a focus on legal data processing and protecting the rights of Data Subjects. The people who take part will learn a lot about the different aspects of data protection, such as

Time Allocated: 20 mins



Determining the Balance Between Data Privacy and Fulfilling the Demands of the Business

1.2.1 Learning Objectives

Upon completion of Topic 2 "Determining the balance between data privacy and fulfilling the demands of the business"

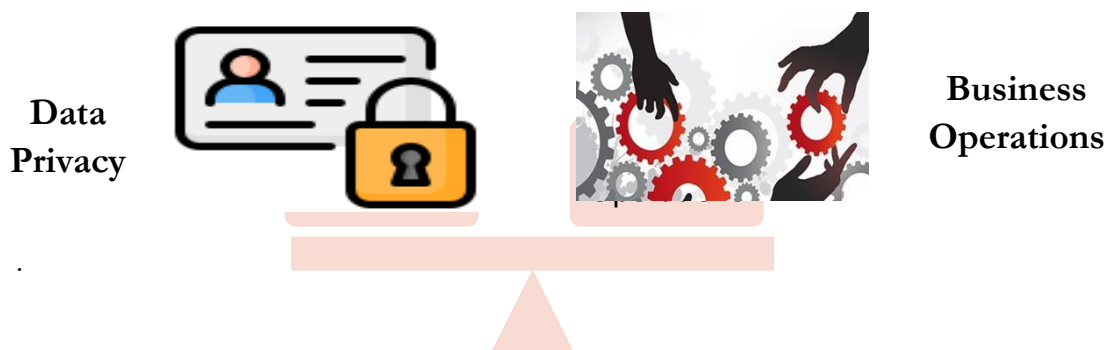
- Understand how to balance data privacy with business requirements.
- The ability to use what you've learned to analyse real-life situations, which lets you quickly find legal reasons, handle requests from data subjects, and make smart decisions.
- Comprehensive strategy of data privacy in business



Determining the Balance Between Data Privacy and Fulfilling the Demands of the Business Operations

1.2.2 Balancing Data Privacy and Business

Determining the Balance Between Data Privacy and Fulfilling the Demands of the Business" refers to finding the right harmony between protecting individuals' data privacy and meeting the operational needs of a business. It involves ensuring compliance with data protection regulations while allowing the business to operate effectively and responsibly with data.



Finding the right balance between data privacy and meeting the business's operational needs is a crucial challenge in today's data-driven world. While safeguarding individuals' privacy rights is a legal and ethical imperative, businesses also rely on data for various purposes, including decision-making, improving customer experiences, and achieving their goals. This delicate equilibrium requires a thoughtful approach that respects privacy regulations and promotes responsible data practices while still allowing organizations to function effectively.

Giving people the knowledge they need about data privacy isn't just a matter of following the rules; it's about giving individuals control again. Personal information has never been more important to keep safe in the digital world we live in now. It is important that data subjects know how their data is handled, processed, and kept safe. This is both their right and duty.



Determining the Balance Between Data Privacy and Fulfilling the Demands of the Business Operations

1.2.3 Comprehensive Strategies for Data Protection and Privacy in Business

Let's look at some important rules and habits that you must follow to protect your privacy and make sure your data is handled in an honest and trustworthy way.



Comprehensive Strategies for Data Protection and Privacy in Business

To achieve this balance, businesses can consider several key strategies must adopted to safeguard personal identifiable information.

- **Data Minimization:** Collect and retain only the data that is strictly necessary for your business purposes. This reduces the potential risk to individuals' privacy while still meeting essential operational needs.
- **Transparency:** Be open and clear about how data is collected, used, and shared. Inform individuals about your data practices, and ensure they have the option to provide or withhold consent.
- **Consent Management:** Implement robust consent mechanisms to obtain explicit permission from individuals when necessary. Ensure that individuals can easily withdraw their consent at any time
- **Data Security:** Invest in strong data security measures to protect sensitive information from breaches and unauthorized access. This not only safeguards privacy but also builds trust with customers.

- **Data Governance:** Establish internal policies and procedures for handling data, including appointing a Data Protection Officer (DPO) if required. Regularly audit and update these practices.
- **Education and Training:** Train employees on data protection and privacy principles to foster a culture of responsibility and compliance within the organization.
- **Privacy by Design:** The concept of Privacy by Design pertains to a data protection strategy that prioritises the incorporation of privacy considerations during the initial stages of product, system, and process development. Integrate privacy considerations into the design of systems, products, and services from the outset, rather than as an afterthought.
- **Data Impact Assessments:** In the context of data privacy regulations such as the NDPA and GDPR, an organisation can use a structured process called a Data Impact Assessment (DPIA) to assess and manage potential risks to individuals' privacy arising from the processing of personal data.
- Conduct Data Protection Impact Assessments (DPIAs) to evaluate and mitigate the risks associated with data processing activities.
- **Third-Party Vendors:** Assess the data practices of third-party vendors and partners to ensure they align with your privacy commitments.
- **Data Retention Policies:** Data retention policies are the rules that companies use to decide how long they will keep and store different kinds of data, like electronic or paper records, documents, and information.
- Develop and adhere to data retention and disposal policies to limit the storage of data for longer than necessary.
- **Incident Response Plans:** Prepare for data breaches by having a robust incident response plan in place. Timely and transparent communication is critical during a breach.
- **Compliance Monitoring:** Keep abreast of evolving privacy regulations and adjust your practices accordingly. Ensure your business is compliant with all relevant laws.
- **Privacy Advocacy:** Consider establishing a privacy advocacy board or committee to provide guidance on privacy-related decisions and policies.



Determining the Balance Between Data Privacy and Fulfilling the Demands of the Business Operations

1.2.4 Challenges Faced by Businesses in Compliance with Data Privacy principles.

Let's look at some important common challenges that businesses face on their pursuit of compliance with these data privacy principles, as well as the potential consequences of non-compliance



..



Challenges Faced by Businesses in Compliance Data Privacy principles and their consequences.

Data Security: Companies often gather and keep private customer data like passwords, personal information, and payment information. It is always hard to keep this data safe from breaches, hacking, or people who shouldn't have access to it.

Recommendations: Implement encryption, software updates, and employee training to protect sensitive data from breaches and unauthorized access

Consent Management: It can be hard to get clear and informed consent for data collection and processing, especially for marketing purposes, because of the many rules that apply and the need to make sure that users really know what they're agreeing to.

Recommendation: Design clear and user-friendly consent forms, offering opt-in and opt-out choices, to ensure informed consent for data processing

Data Minimization: It's always hard to find the right balance between collecting just enough data for business purposes and not collecting too much personal data. Over-collection can make people worry about their privacy.

Recommendation: Audit data collection, use anonymization, and educate staff to balance business needs with privacy concerns

Compliance Across Jurisdictions: Businesses that do business around the world have to deal with different data protection laws and rules, which often have complex requirements.

Recommendations:

Employ contractual clauses and compliance frameworks to navigate varying international privacy laws and regulations and

Appoint a Data Protection Officer, develop a flexible compliance program, and stay updated with evolving regulations worldwide.

Data Retention: It can be hard to figure out how long to keep different kinds of data, especially when there are different business needs and regulatory requirements. It can be bad for your privacy to keep data for too long.

Recommendations: Establish a retention policy, automate data archiving, and maintain records for compliance and regular review

Data Portability: Some laws say that people must be able to access and move their data to other service providers. To make this possible, technical solutions are needed and interoperable data formats must be followed.

Recommendations: Create user-friendly tools for data access and transfer, use interoperable formats, and ensure secure data transfer

Data Subject Rights: It can be hard to keep track of and respond to requests from data subjects for things like access, correction, or deletion within the time limits set by law.

Recommendation: Implement a dedicated request management system, train staff, and adhere to legal response timeframes

Data Impact Assessments: It's hard to do privacy impact assessments to find and reduce the privacy risks that come with new technologies or ways of processing data. This is because they are procedural and need expert knowledge.

Recommendations: Train staff in Privacy Impact Assessments (PIAs), develop templates, and ensure PIAs are conducted for relevant projects

Data Breach Response: Being ready for and responding to data breaches is very important for keeping people safe and the company's reputation from getting hurt.

Recommendations: Develop an incident response plan, define roles, and regularly test it through simulations for effective breach response



Consequences of Non-Compliance with Data Privacy Regulations in Nigeria

As a DPO, it is important to note this:

Legal Consequences: Failure to comply with Nigerian data privacy laws, such as the Nigeria Data Protection Act, 2023 (NDPA), can result in legal penalties and fines. The NDPA, for example, states that "The "higher maximum amount" shall be the greater of — (a) N10,000,000, and (b) 2% of its annual gross revenue in the preceding financial year. (5) The "standard maximum amount" shall be the greater of — (a) N2,000,000, and (b) 2% of its annual gross revenue in the preceding financial year"

Financial Consequences: Failure to comply can result in significant financial losses. Aside from fines, businesses may face legal fees, remediation costs, and civil litigation from affected individuals. Dealing with the fallout from noncompliance, such as responding to data breaches, addressing regulatory investigations, and implementing corrective actions, can disrupt normal business operations, resulting in decreased efficiency and productivity.

Customer Trust: As people become more concerned about the privacy of their data, noncompliance can erode trust. Customers may lose faith in a company's ability to safeguard their personal information, resulting in lower customer loyalty and potential business decline.

Loss of Competitive Advantage: A reputation for strong data privacy practices can be a significant advantage in a competitive market. Noncompliance can erode this advantage, hampered business growth, and hampered market competitiveness.

Costs of Audits and Investigations: Noncompliance may result in regulatory audits and investigations, which can be time-consuming and expensive. Businesses may need to set aside resources to respond to inquiries and provide proof of compliance.

Interactions and Discussions 1



Scenario 1

Time Allocated: 15 mins

In the next 10 minutes, we will collectively address a practical challenge related to data privacy compliance. Please read through the background scenario provided, which describes a situation involving employee data access at a technology firm. You will take on the role of a Data Protection Officer (DPO) at the company.

Employee Data Access

Background: You are the data protection officer (DPO) at a medium-sized technology firm. Employee data is collected and stored by the company for HR and operational purposes. You recently received a request from the human resources department to grant them access to all employee data, including personal contact information, performance reviews, and medical records. They claim that having access to this data will allow them to make more informed decisions about promotions and job assignments.

Challenge:

The task at hand is to evaluate the situation in terms of data privacy compliance. What are the potential compliance issues, and how can you address them while balancing HR needs with data protection requirements? **(15 min discussion)**

Scenario 2: Question and Answer

All participants will attempt the below question (5 min discussion)

E.g. Data Security:

What happens if a small healthcare clinic stores patient records on a computer and a hacker gains access, stealing patient data?

Answer: If a small healthcare clinic stores patient records on a computer and a hacker gains access, the consequences can be severe. The stolen patient data could lead to privacy breaches, identity theft, and compromised medical information, putting patients at risk. Additionally, the clinic may face legal and financial repercussions, damage to its reputation, and the need for costly security improvements to prevent future breaches.

Q1: Consent Management:

What happens if a mobile app wants to access a user's location for personalised recommendations without first ensuring that the user understands and agrees to this before using the app?

Q2: Data Subject Rights:

What are the potential legal ramifications if an online retailer fails to comply with a customer's request to delete their account within a reasonable timeframe?





Tips for Trainer

- Assess the baseline knowledge of the audience regarding data protection principles to tailor the delivery to their level of understanding.
- Clearly communicate the learning objectives at the beginning of the session to help participants understand what they will gain from the discussion.
- Emphasize the critical role data protection plays in safeguarding sensitive information and maintaining trust with stakeholders.
- Provide clear and concise definitions of data protection and data privacy to establish a foundational understanding for participants.
- Demystify the key principles outlined in the Nigeria Data Protection Act to ensure participants grasp the legal framework.
- Illustrate data protection principles with practical examples and real-world scenarios to enhance comprehension and application.
- Create an environment for open discussions, allowing participants to share insights and experiences related to data protection.
- Highlight common challenges faced by businesses in complying with data privacy principles and discuss strategies to overcome them.
- Emphasize the potential consequences of non-compliance with data privacy regulations, including legal, financial, and reputational risks.
- Show how achieving a balance between data privacy and business demands contributes to long-term business sustainability.
- Discuss a thorough overview of strategies businesses can adopt to ensure comprehensive data protection and privacy practices.
- Discuss emerging challenges that businesses may face in the evolving landscape of data protection and privacy.
- Integrate relevant case studies to illustrate successful implementations of data protection strategies and the lessons learned.
- Emphasize the importance of ongoing learning in the dynamic field of data protection, prompting participants to stay informed about updates and changes.
- Allocate time for questions and answers to address any uncertainties or queries participants may have, promoting a deeper understanding of the material.

SECTION 2

The Crucial Role of the Data Protection Officer (DPO)

Topic 1

Defining the Responsibilities and Functions of Data Protection Officers (DPOs)

Under this topic, the following key areas shall be discussed:

- 2.1 Learning Objectives
- 2.2 Who is a Data Protection officer (DPO)
- 2.3 Defining the Responsibilities and Functions of Data Protection Officers
- 2.4 Frequently asked question on the appointment of a Data Protection Officers
- 2.5 Interactive session

Within this section, we will explore the “Defining the Responsibilities and Functions of Data Protection Officers (DPOs),” you would be learning about the key aspects related to the role and duties of Data Protection Officers (DPOs) in the context of the Nigeria Data Protection Act, 2023. The section would likely cover the following topics:

Time Allocated: 20 mins



Defining the Responsibilities and Functions of Data Protection Officers (DPOs)

2.1 Learning Objectives

Upon completion of Topic 1 “Defining the Responsibilities and functions of Data Protection Officers (DPOs)”

- An introduction to the who a Data Protection Officer (DPO)
- The crucial role of Data Protection Officers and their significance in ensuring data protection and compliance with data privacy laws and regulations.
- Cultivate a Skill Set for Effective DPOs.





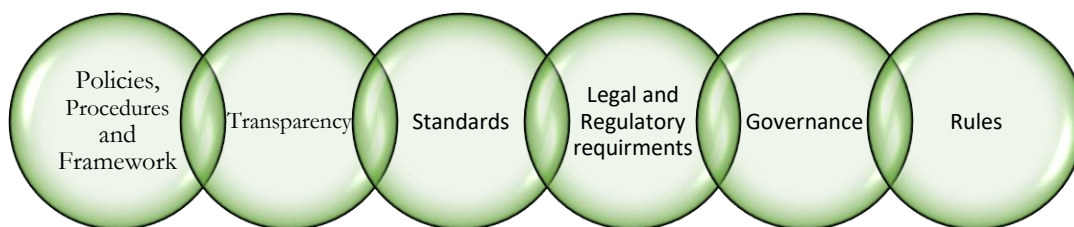
Defining the Responsibilities and Functions of Data Protection Officers (DPOs)

2.2 Who is a Data Protection Officer (DPO)

Data Protection Officer (DPO) is an individual appointed by an organization as their company's data guardian.



Data Protection Officers (DPOs)



In this session we would be looking into the following sessions as seen below

- Who is a DPO
- Why is a DPO assigned?
- Who needs a DPO?
- Why Does an Organisation Require a DPO?
- How is a DPO assigned?
- Important of appointing a DPO
- Characteristics of a DPO



Who is a DPO?

A Data Protection Officer (DPO) is an individual or entity appointed by an organization to oversee and ensure compliance with data protection laws and regulations. The specific roles and responsibilities of a DPO can vary depending on the legal requirements of the country or region, as well as the organization's needs.

The DPOs acts as a connector between data protection authorities and data subjects, providing guidance on data protection issues, conducting out data protection impact assessments, and ensuring compliance with data protection rules. The Data Protection Officer (DPO) has a crucial responsibility in protecting the privacy and rights of individuals in relation to the processing of data.



Why is a DPO assigned?

DPOs are appointed based on their knowledge of data protection laws and practises. They have an in-depth understanding of privacy regulations and can advise the organisation on how to remain in compliance. DPO's must operate independently and without conflicts of interest. Because of this independence, they can make judgements only in the best interests of data subjects and data protection.

N.B The primary point of contact for data subjects and supervisory agencies is the DPO. This means that individuals can contact the DPO if they have issues or concerns about their personal data.



Who needs a DPO?

Several privacy regulations, such as The Nigeria Data Protection Act (NDPA) and General Data Protection Regulation (GDPR) in the European Union, indicate that businesses must appoint a DPO. But based on the jurisdiction, the specific conditions under which a business must appoint a DPO may be slightly different. In most cases, businesses that meet any of the following requirements must hire a DPO:

Public Authorities: Regardless of the type of data processed, public authorities and governmental entities are normally required to appoint a DPO. Like the financial institutions eg Banks

Organisations that Process Personal Data on a Large Scale: If an organisation processes personal data on a large scale, they are likely required to have a DPO. The term "large-scale processing" is rather ambiguous and depends on the context. It could, for example, relate to the amount of data processed or the number of data subjects e.g. Telecommunication companies

Processing Sensitive Data: Organisations that process particularly sensitive categories of data, such as health information, racial or ethnic origin, political ideas, religious beliefs, biometric data,

or data relating to criminal convictions, are frequently required to designate a DPO e.g., Health care providers, HMO companies, hospitals etc

Regular and Systematic Monitoring: Organisations that conduct large-scale regular and systematic monitoring of data subjects, such as online behaviour tracking, must have a DPO. E.g., E-commerce platforms

Cross-Border Data Processing: If a company works in multiple EU member states and processes data across borders, it may need to employ a DPO. E.g., Government agencies

Legal Requirement: Even if an organisation does not meet the criteria, some jurisdictions may impose legal requirements necessitating the appointment of a DPO. Educational institutions like schools, universities etc

Why Does an Organisation Require a DPO?

A Data Protection Officer (DPO) is needed because it's a legal requirement, especially in places Nigeria, United State, Canada, and the European Union, it's challenging to keep track of all the personal data that people share online these days. The DPO makes sure that organisations follow the law, helps them understand the complicated rules about data security, and is very important for lowering the risks that come with data breaches and privacy violations. In addition to meeting legal requirements, a DPO help builds trust by showing that an organisation is dedicated to protecting data. This makes customers, partners, and other stakeholders more likely to trust the organisation.

How is a DPO assigned?

A Data Protection Officer (DPO) is chosen based on a number of important factors, such as the needs of the organisation, the law, and the type of data controlling and processing that is being done. The following are popular ways to give someone a DPO:

- A DPO must be appointed by some places because of data protection laws, like the Nigeria Data Protection Act, 2023 and the General Data Protection Regulation (GDPR). This rule applies to groups that deal with private information, process a lot of data, or are government agencies.

- Companies can choose to hire a DPO even if they are not forced to by law. This can help them improve their data protection methods, show they care about data privacy, and understand the complicated privacy rules.
- It's important to know what kind of data processing an organisation does and how big it is. It is usually a good idea for organisations that deal with a lot of personal data or sensitive information to hire a DPO to make sure that data security standards are met.
- The need for a DPO can also be caused by the complexity of an organization's data environment, such as the amount and types of data it has. Keeping data safe and private in complex data environments might need a specialised expert.
- Companies may hire a DPO to build trust and meet the needs of customers, partners, and stakeholders. Showing that you care about data security can give you an edge over your competitors.



Important of appointing a DPO:

- The DPO plays a key role in making sure that the company follows data security laws. By following the rules, they help the organisation escape expensive fines and legal problems.
- DPOs help people use their rights to protect their own data. This includes the right to see their data, ask for changes to be made to it, or even have it deleted.
- Through the idea of "privacy by design," DPOs urge companies to include privacy in their systems, products, and services from the start, instead of adding it as an afterthought.
- If there is a data breach, the DPO oversees organising the company's response and making sure that the people whose data was compromised are informed right away and that the right steps are taken.
- It is the job of the DPO to teach employees about data security principles and best practises. They help the organisation develop a mindset of responsibility and following the rules.
- Having a DPO shows customers and partners that the company cares about their privacy. This can help you beat the competition and build trust.



Characteristics of a DPO:

In most cases, the following are characteristics of a DPO:

- A DPO should have a solid grasp of the data protection legislation and best practises in place in their jurisdiction.

- They should work without any conflicts of interest and independently to ensure that they are able to make judgements that are in the best interest of the people whose data they are analysing.
- The DPO should make themselves available to data subjects and supervisory authorities for the purpose of fielding questions and addressing concerns.
- They offer the company guidance on how to handle concerns pertaining to data protection and privacy.
- Ensures that the organisation complies with the many laws and regulations concerning the protection of personal data.
- DPOs encourage transparency on the activities that include the processing of personal data.
- They promote the organization-wide discussion of ethical issues relating to the use of data and the protection of personal information.
- DPOs play a role in holding the organisation accountable for data protection compliance and play a role in holding the organisation accountable.
- They may have applicable qualifications or training in data protection and have received education in this area.
- Pays close attention to the details to preserve sensitive data. Here is an overview of the typical roles and responsibilities of a DPO.



Define the Responsibilities and Functions of Data Protection Officers (DPOs)

2.3 Defining the Responsibilities and Functions of Data Protection Officers (DPO)

The roles and responsibilities of a Data Protection Officer (DPO) across various data protection principles.



What are the crucial roles and responsibilities of a DPO?

In Nigeria, the role and responsibilities of a DPO are primarily defined by the Nigeria Data Protection Act (NDPA). These regulations were enacted to ensure the protection of personal data in Nigeria and establish the framework for data protection.

Under the NDPA, the responsibilities of a DPO include, but are not limited to:

- The DPO is responsible for providing advice to the Data Controller and Data Processor, as well as their employees, regarding compliance with the NDPR and NDPA. They offer guidance on how to handle personal data in accordance with the law.
- The DPO is tasked with monitoring the organization's compliance with the NDPA and related data protection policies. They ensure that data processing activities are carried out in accordance with the law and established procedures.
- The DPO may be involved in conducting or overseeing Data Protection Impact Assessments to identify and address risks associated with specific data processing activities.

- The DPO plays a role in educating and raising awareness among employees about data protection laws and best practices. This includes providing training and guidance to ensure that all staff members understand their obligations in safeguarding personal data.
- The DPO serves as a contact point for data subjects, addressing their requests and inquiries related to their personal data. They ensure that individuals' rights under data protection laws are respected.
- In the event of a data breach or other data protection incidents, the DPO is responsible for reporting to the relevant data protection authority in accordance with the NDPA requirements.
- The DPO encourages and promotes a culture of privacy by design and by default within the organization, advocating for the integration of data protection principles into product and system development.
- DPOs may be involved in developing, reviewing, and updating the organization's data protection policies, procedures, and documentation to ensure continued compliance with the NDPA.
- The DPO oversees the organization's relationships with data processors and third-party vendors, ensuring that these parties adhere to data protection laws and regulations.
- DPOs may be involved in resolving conflicts and disputes related to data protection within the organization.
- When a data breach occurs, the DPO is responsible for organising the company's reaction. This includes assembling an incident response team comprised of IT professionals, legal specialists, and communication specialists.
- The DPO may be required to inform the appropriate data protection authority of the breach, depending on local rules. The DPO is responsible for making sure the notification is sent out in a timely manner and has all the required details.
- Managing notifications and registrations with the appropriate data protection authority in accordance with the data controller's data processing activities is the primary duty of the DPO.
- Additionally, the Data Protection Officer is responsible for maintaining these registrations and notifications current.



2.4 Here are the answers to some frequently asked questions regarding the appointment of a Data Protection Officer (DPO) in Nigeria:

1. Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances:

The appointment of a Data Protection Officer is mandatory in certain circumstances in Nigeria. According to Section 32 of the Nigeria Data Protection Act (NDPA), a Data Controller of Major Importance must designate a DPO with expert knowledge of data protection law and practices. In addition to this, Regulation 4.1 of the Nigeria Data Protection Regulation (NDPR) and Section 3.4.1 of the Implementation Framework mandate every Data Controller to designate or appoint a DPO for ensuring adherence to the NDPA, relevant data privacy instruments, and data protection directives of the Data Controller. Furthermore, specific categories of Data Controllers, such as government entities, those processing a large volume of personal data, those processing sensitive personal data, and those that possess critical national information infrastructure, are required to appoint a dedicated DPO.

2. What are the sanctions for failing to appoint a Data Protection Officer where required?

Sections 48 and 49 of the NDPA provide that the NDPC may impose fines in respect of a breach of the provisions of the NDPA which also includes failing to appoint a DPO. The range of fines imposed under the NDPA are as follows:

- in the case of a Data Controller or Data Processor of Major Importance, the payment of a fine of 2% of the organisation's annual gross revenue of the preceding year or the payment of the sum of 10 million Naira, whichever is greater; and
- in the case of a Data Controller or Data Processor not of Major Importance, the payment of a fine representing 2% of the organisation's annual gross revenue of the preceding year or payment of the sum of 2 million Naira, whichever is greater

3. Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The protection of a DPO from disciplinary measures or employment consequences would depend on the terms of their employment contract or any service contract. The NDPA and NDPR do not explicitly address this aspect.

3. Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, a business may appoint a single DPO to cover multiple entities. However, section 3.5 of the Implementation Framework stipulates that a Nigerian subsidiary of a multinational company should appoint a Nigerian-based DPO. This local DPO may report to a global DPO, if one exists.

4. Please describe any specific qualifications for the Data Protection Officer required by law.

Section 32(3) of the NDPA provides specific qualifications for a DPO, which include:

- Having professional expertise in Nigerian data protection laws and practices.
- An in-depth understanding of applicable data protection laws.
- Knowledge and skills to inform and advise the organization, monitor compliance, assign responsibilities, raise awareness, advise on data protection impact assessments, and liaise with data protection authorities on data protection matters.
 - inform and advise the organisation, management, employees and third-party processors of their obligations under the NDPA;
 - monitor compliance with the NDPA and with the organisation's own data protection objectives;
 - assign responsibilities, raise awareness and train members of staff involved in Personal Data processing activities and operations;
 - advice on data protection impact assessment and monitor its performance; and
 - liaise with the NDPC and/or the DPCO on data protection matters

5. What are the responsibilities of the Data Protection Officer as required by law or best practice?

The responsibilities of a Data Protection Officer, as outlined in the NDPA and NDPR, include advising the Data Controller or Data Processor, monitoring compliance, acting as the contact point for data protection authorities, informing and advising the organization, training staff, advising on data protection impact assessments, and liaising with data protection authorities on data protection matters.

6. Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, it is not mandatory to notify the Nigeria Data Protection Commission (NDPC) when an organization appoints a DPO.

7. Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Yes, according to Regulation 3.1(7) of the NDPR, the identity and contact details of the DPO must be included as part of the information that a Data Controller is required to provide to Data Subjects before collecting their Personal Data. Therefore, the DPO should be identified in the Data Controller's privacy policy, notice, or any equivalent document made available

Let's Attempt these questions in (5minutes)

1. What is the primary responsibility of a Data Protection Officer (DPO) within an organization?
 - a) Managing social media accounts
 - b) Ensuring compliance with data protection laws and regulations
 - c) Handling customer complaints
 - d) Conducting market research

2. What does the term "Data Subject" refer to in data protection terminology?
 - a) An individual whose personal data is being processed
 - b) A computer server
 - c) A data controller
 - d) A legal document

3. What is the significance of a Data Protection Impact Assessment (DPIA) in data protection practices?
 - a) Monitoring network traffic
 - b) Creating marketing campaigns
 - c) Identifying and mitigating risks associated with specific data processing activities
 - d) Managing office supplies

Interactions and Discussions 2

(Assignment)



Case Study

For this assignment, you will analyse a real-world scenario involving "GUZZY Bank," a well-established financial institution in Nigeria, which recently experienced a data breach. Your task is to answer the following questions based on the scenario:

This assignment would be discussed for the commencement of day 2 session.

Response to a Data Breach at a Nigerian Financial Institution

The GUZZY Bank in Nigeria is a well-established financial institution that manages the sensitive financial information of thousands of consumers. The bank employs a Data Protection Officer (DPO) charged with ensuring compliance with the Nigeria Data Protection Act (NDPA).

The Data Breach: One morning, the bank's IT department detects peculiar server activity. After conducting an exhaustive investigation, they corroborate that a data breach has occurred. Customer data, including account information and contact details, has been compromised.

From the case study above, make reference to the scenario and provide answers to the below questions

Questions:

- What steps should the DPO perform immediately after learning of the data breach?
- How would you communicate with the impacted customers?
- Which regulatory requirements must be fulfilled in this circumstance?

Time Allocated: 30 minutes





Tips for Trainer

- Ensure that the learning objectives are clearly aligned with the content, providing participants with a roadmap for what they will gain from the session.
- Clearly define the roles and functions of Data Protection Officers (DPOs), emphasizing their crucial responsibilities within an organization.
- Identify and discuss key characteristics that define an effective DPO, providing participants with a clear understanding of the qualities required for the role.
- Address frequently asked questions regarding the appointment of a DPO, covering common queries and concerns that organizations may have in the context of Nigeria's regulations.
- Foster an interactive session, encouraging active participation through discussions, Q&A, and case studies to enhance engagement and knowledge retention.
- Illustrate the responsibilities of DPOs with practical examples and real-world scenarios, allowing participants to grasp the application of concepts in different contexts.
- Provide a comprehensive understanding of legal requirements surrounding the appointment and functions of DPOs, ensuring participants are well-versed in regulatory compliance.
- Explore practical challenges that DPOs may encounter in fulfilling their roles and discuss effective strategies for overcoming these challenges.
- Specifically, focus on frequently asked questions related to appointing a DPO within the context of Nigerian regulations, offering clarity on compliance requirements.
- Incorporate relevant case studies for participants to analyze, linking theoretical knowledge to practical applications in the realm of DPO responsibilities.
- Offer additional resources and references for participants seeking a deeper understanding of the DPO role, such as relevant guidelines, articles, or legal frameworks.
- Create opportunities for participants to share their experiences or insights related to DPO roles, fostering peer-to-peer learning within the training session.
- Integrate interactive quizzes or polls to gauge participant comprehension and reinforce key concepts in an engaging manner.
- Tailor discussions to address industry-specific nuances in the role of DPOs, ensuring relevance for participants from various sectors.
- Allow time for questions at the end of the session, enabling participants to internalize key takeaways and consider how the insights apply to their specific organizational context.

z

SECTION 3

Duties of Data Processors and Controllers

Topic 1

In-depth understanding of the Roles of Data Processors and Controllers

Under this topic, the following key areas shall be discussed:

- 3.1.1 Learning Expectations
- 3.1.2 Introduction to data controller and data processor
- 3.1.3 Roles and Responsibilities of a data controller and data processor
- 3.1.4 Obligations of a data controller and data processor

Under this training topic, the participants will gain full understanding of the roles, responsibilities, and legal obligations of data processors and controllers in terms of data protection and privacy. Participants will learn about the important functions, compliance requirements, and best practices that govern the responsible management of personal data. By the end of this training, you will have the knowledge and tools you need to make sure that personal data are handled in a safe and legal way.

Time Allocated: 15 mins



In-depth understanding of the Roles of Data Processors and Controllers

3.1.1 Learning Objectives

Upon completion of Topic 1 “In-depth understanding of the roles and data processors and controllers, participants shall be equipped with the skills to:

- Understand the definition of a data controller and a data processor.
- Understand the Roles of Data Processors and Controllers of Data Protection and Privacy Principles
- Differentiate between the roles and responsibilities of data processors and data controllers.

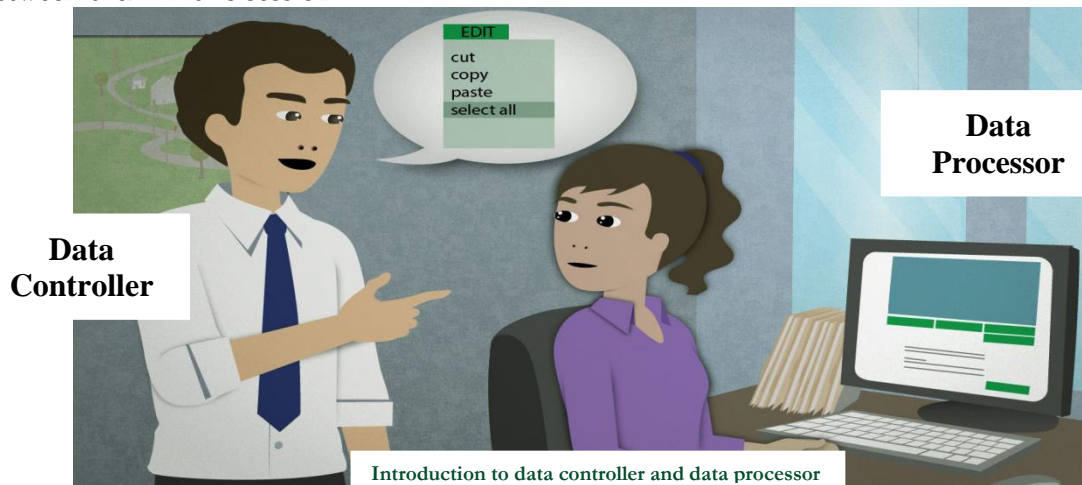




In-depth understanding of the Roles of Data Processors and Controllers

3.1.2 Introduction to Data Controller and Data Processor

In the context of data privacy and protection, the roles of data controllers and processors are essential. We will go into great detail about these jobs, their duties, and the important differences between them in this session



There are two important roles in the world of data protection: Data Controllers and Data Processors." When it comes to personal data, Data Controllers are like the "captains" who guide the ship and decide what to do. The Data Processors, on the other hand, are like the "crew" and are in charge of doing what the Controller says. Let's take a closer look at these jobs, starting with what they mean



Who is a Data Controller and a Data Processor

Data Controllers: A data controller is a person or organisation that decides how and why to handle personal data. In simpler terms, they decide what personal information is gathered and how it is used. Data controllers are in charge of making sure that personal data is handled in a way that follows data security laws and respects the rights of data subjects, or the people whose data it is about. This can include businesses, groups, or people who gather and use personal information for specific reasons.

Example; Data Controller: A principal of a school who keeps track of students' personal data, including names, addresses, and attendance logs, in order to make decisions regarding their education

Data Processors: On the other hand, data processors are businesses or people that handle personal data for data managers. They do certain jobs that have to do with processing data, but they don't decide what the processing is for or how it is done. Data processors follow the directions given by data controllers and are usually hired through agreements or contracts. It is their job to make sure that the data is handled safely, in line with the law, and according to the data controller's instructions.

Example: A data processor is a teacher employed by the school who maintains student attendance records in accordance with directives from the principal, but who does not decide on the purpose or use of the data acquired.

To ensure that personal data is treated lawfully, safely, and openly, data controllers and processors have related but separate duties to perform. Processors deal with the how of data processing, whereas controllers specify the what and why. Their collaboration is necessary to ensure privacy compliance and data protection.

For personal data to be handled responsibly, the roles of data processors and controllers are essential. An outline of their significance is given below:

Data Controllers:

Legal Responsibilities: It is the legal responsibility of data controllers to guarantee that personal data is processed in accordance with data protection laws and rules, including the Nigeria Data Protection Act, 2023 (NDPA). This entails securing legitimate permission and defending the rights of individuals.

Privacy Protection: By deciding why and how to process personal data, controllers are essential in protecting the privacy of persons. They have to have policies in place to guard against data breaches and guarantee data security.

Transparency: Data controllers are in charge of giving data subjects easily understandable information about the reasons, legal justifications, and durations for which their data is handled. Individuals gain trust when there is transparency.

Rights of Data Subjects: Controllers are required to assist individuals in exercising their rights, which include the ability to access, correct, or remove personal information. They must also reply to requests from data subjects in a timely manner and within the bounds of the law.

Data Processor:

Expertise in Data Processing: Data processors are equipped with certain skills and experience in data processing. Their knowledge is crucial for effectively processing and managing data in accordance with controller directives.

Data Security: To protect personal data, processors put organisational and technical safeguards in place. This helps shield data from breaches and unwanted access. It also includes encryption, access controls, and routine security audits.

Data Protection Compliance: By abiding by legal requirements, upholding data processing agreements, and collaborating with supervisory agencies, processors help controllers comply with data protection legislation.

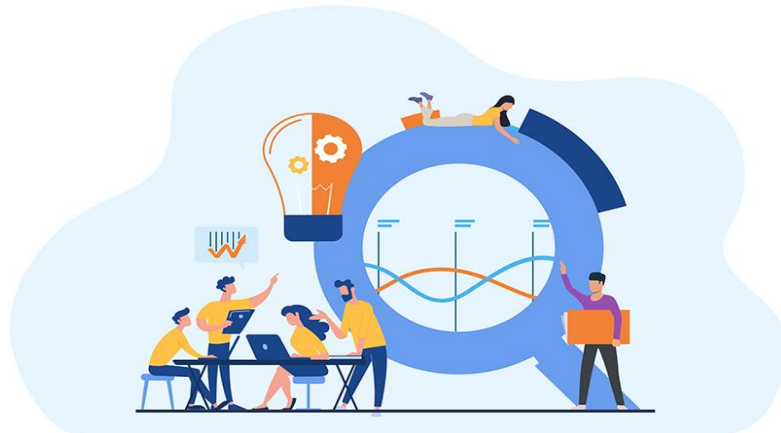
Effective Data Management: By guaranteeing that data is accessible and available when requested, data processors assist controllers in effectively managing and processing data. This helps ensure that organisations run smoothly.

Support for Data Subject Rights: Processors help controllers rapidly react to requests from data subjects. They have to work with the controller to make it easier for data subjects to exercise their rights.



In-depth understanding of the Roles of Data Processors and Controllers

3.1.3 Roles and Responsibilities of a Data Controller and Data



The purpose and method of data processing are decided by controllers, while processors carry out these tasks in accordance with directives.



Relationship between Data Controller and Data Processors

The purpose and method of data processing are decided by controllers, while processors carry out these tasks in accordance with directives. Each party is required to maintain data confidentiality and privacy, and their relationship is regulated by a legal agreement that guarantees adherence to data protection regulations.

Data Controller:

- **Primary Responsibilities:** Data controllers oversee determining the purposes and means of processing personal data. They choose the objectives behind the collection and processing of data. For example, a business that gathers consumer information for marketing reasons is a data controller since it chooses the marketing tactics and uses the information for.
- **Legal Obligations:** Data controllers are responsible for making sure that all processing operations abide by the rules and legislation pertaining to data protection. They bear the responsibility of securing the requisite consents from individuals who are data subjects and of handling data in a manner that upholds the rights of those individuals.

- **Risk management:** Controllers are responsible for identifying and controlling the risks related to data processing. This entails maintaining data security, reducing data breaches, and swiftly handling occurrences.

Data Processor:

- **Processing on behalf of Controller:** Organisations or other entities that handle personal data *on* behalf of data controllers are known as data processors. They act in accordance with the directives and goals provided by the controller. A data processor would be a cloud service provider that stores customer data on behalf of a business.
- **Compliance with Controller's Instructions:** It is legally required of data processors to process information in a way that closely complies with the controller's instructions. They shall take the necessary security precautions to safeguard the data and refrain from using it for any other reasons.
- **Data Security and Confidentiality:** In order to protect the personal data they are processing, processors need to have security measures in place. This covers protocols such as access controls, encryption, and recurring security audits. They must also keep the data's confidentiality intact.

Agreement for Data Processing (DPA):

The relationship between a data controller and data processor is typically formalized through a Data Processing Agreement (DPA) or a similar legal contract. The DPA outlines the specific terms and conditions under which personal data will be processed

In this agreement, Controllers outline their expectations for processors' handling of personal data in the DPA. It addresses topics including subcontracting, data protection legislation compliance, breach notification, and data security. To make sure that all parties are aware of their respective duties, responsibilities, and legal requirements, the DPA is an essential document. It also serves as a way to prove adherence to data protection laws.

It is important to note that the data processors carry out the processing tasks effectively and securely, whereas data controllers are in charge of decision-making, openness, and general compliance with data protection acts. Both responsibilities are critical to maintaining the legal and

ethical standards in data management as well as safeguarding the privacy of people' data. Their partnership guarantees that sensitive information is handled carefully and ethically.



Distinguishing the roles of data controllers and data processors in a business is essential for several reasons.

- **Legal Compliance:** Defined roles ensure that the organisation complies with data protection standards such as the NDPA, GDPR or other regional laws. Failure to distinguish between these duties might result in legal sanctions and large fines.
- **Accountability** is established by assigning explicit roles to controllers and processors. Controllers determine the purposes and methods of processing, while processors carry out the processing. This accountability is essential for accountable and transparent data management.
- **Transparency** is promoted by a clear delineation between roles, both internally and with data subjects. Data subjects have the right to know who is handling their personal information and why. Transparency fosters customer and stakeholder trust.
- **Risk Management:** Understanding these responsibilities enables firms to analyse and manage data processing risks. Controllers can employ risk mitigation mechanisms, while processors can incorporate data security safeguards.
- **Data Subject Rights:** Understanding the responsibilities allows data subjects to properly exercise their privacy rights. They know who to contact if they want to access, correct, or delete their personal information. Individuals are now able to govern their own information.
- **Efficient Data Processing:** Data processing operations can be handled more efficiently by splitting responsibilities. Controllers can concentrate on strategic decisions while processors tackle technical aspects of data management.
- **Data Security:** When responsibilities are clearly defined, businesses can adopt suitable data security measures. Processors, in particular, are accountable for data security, which is critical for preventing breaches and safeguarding sensitive data.

- **Contractual Clarity:** Defining these roles in unambiguous contracts or agreements creates a formal framework for data management. It ensures that all parties understand their roles and responsibilities.
- **Organisational Efficiency:** Role separation improves organisational efficiency. Each party can focus on its primary functions, resulting in a smoother workflow and improved resource utilisation.



The relationship between the Roles and Responsibilities of and Data Controller and Data Processors.

To protect personal data's security and privacy, here are some crucial roles and responsibilities of their data controller and processor:

Data Controller: Playing a pivotal function, the data controller is in charge of deciding how and why personal data is processed. They have to keep track of everything, make sure it's secure, and handle data breaches.

Data Processor: Data processors handle personal data processing on behalf of data controllers. They have to uphold security, comply with the data controller's orders, and support data breach notification.

Data Protection Officer (DPO): The DPO is responsible for monitoring NDPA adherence inside a company. They function as a point of contact for data subjects and regulatory bodies, monitor compliance, and offer advice on privacy-related issues.

Responsibility	Data Controller	Data Processor
Determining Data Processing Purposes	Defines why and how personal data is collected and processed, specifying purposes.	Carries out data processing activities based on the controller's instructions.
Legal Compliance	Ensures data processing activities comply with data protection laws.	Implements processing activities as per controller's instructions and legal requirements.

Consent Management	Obtains and manages consent from data subjects when required.	Supports the controller in managing and recording consent.
Data Minimization	Collects and processes only necessary personal data, avoiding excess collection.	Processes data as instructed, avoiding unnecessary data collection.
Data Subject Rights	Recognizes and facilitates data subjects' rights, such as access and rectification.	Assists in responding to data subject requests for access or correction.
Security and Data Protection	Implements security measures to protect data from breaches and unauthorized access.	Implements technical and organizational security measures to safeguard data.
Risk Management	Identifies and mitigates risks associated with data processing.	Assists in risk assessment and mitigation in data processing.
Data Impact Assessments	Conducts Data Protection Impact Assessments (DPIAs) to identify and mitigate privacy risks.	Assists in providing information for DPIAs and ensuring risk reduction.
Record Keeping	Maintains records of data processing activities, including purposes and retention periods.	Maintains records of processing activities carried out on behalf of the controller.
Data Subject Communication	Handles inquiries and requests from data subjects regarding their data.	Provides information to data subjects as directed by the controller.
Legal	Supports compliance with data protection laws.	Assists in ensuring compliance with data protection laws.



3.1.4 Obligation of the Data Controller and the Data Processor in alignment to the Nigeria Data Protection Act (NDPA)

The Nigeria created the Data Protection Act (NDPA) framework to ensure data privacy and protections, Complying with the NDPA and guaranteeing the protection of personal data requires an understanding of the various roles and duties of these parties

Controller	Data Processor	Data Protection Officer (DPO)
Determine the purpose and means of data processing in compliance with NDPA requirements.	Process personal data only on the documented instructions of the data controller.	Act as an independent advisor on NDPA compliance.
Obtain valid consent when required and maintain records of processing activities.	Implement security measures to protect data as required by NDPA.	Monitor compliance with NDPA and internal data protection policies.

Appoint a Data Protection Officer (DPO) if necessary and ensure their independence.	Assist the data controller in notifying the NDPC and data subjects in case of data breaches.	Provide guidance on Data Protection Impact Assessments (DPIAs) and ensure their completion.
Implement appropriate data security measures to protect personal data.	Maintain records of processing activities and cooperate with audits and inspections.	Cooperate with NDPC and act as the contact point for the regulatory authority.
Notify the Nigerian Data Protection Commission (NDPC) of data breaches as per NDPA requirements.	Assist the data controller in fulfilling data subject rights requests.	Train and raise awareness among employees regarding data protection.
Ensure data subjects can exercise their rights under the NDPA.	Ensure the transfer of data complies with NDPA requirements.	Assist in ensuring that data breaches are documented, analyzed, and reported.
Conduct Data Protection Impact Assessments (DPIA) where applicable, particularly for high-risk data processing.	Develop and implement data protection policies and procedures.	Oversee the development and implementation of data protection policies.
Develop and implement data protection policies and procedures.	Regularly review and update data protection policies in line with NDPA changes and developments.	Ensure that data subjects can exercise their rights under the NDPA.
Regularly review and update data protection policies in line with NDPA changes and developments.	Ensure compliance with NDPA in data processing operations.	Ensure that data breaches are documented, analyzed, and reported to the regulatory authority.

Topic 2

Responsibilities of Controllers and Processors in Cases of Subcontracting or Sub-processing

Under this topic, the following key areas shall be discussed:

- 3.2.1 Learning Expectations
- 3.2.2 Defining the Sub-contracting and Sub-processing.
- 3.2.3 Data Controller and Processor in case of the Sub-contracting and Sub-processing
- 3.2.4 Responsibilities of a Data Controller and Processor in case of the Sub-contracting and Sub-processing

Time Allocated: 15 mins



Responsibilities of Controllers and Processors in Cases of Subcontracting or Sub-processing

3.2.1 Learning Objectives

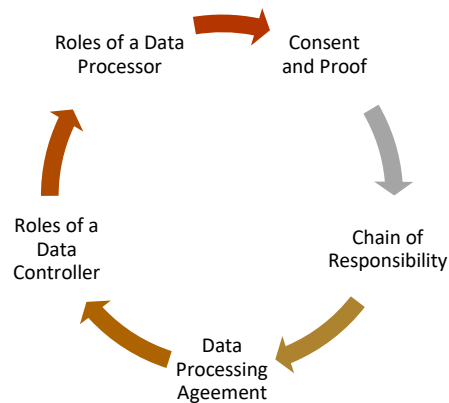
Upon completion of Topic 2 “Responsibilities of Controller and Processors in cases of Sub-contracting and Sub-processing”, participants shall be equipped with the skills to:

- Understand the meaning of a sub-contracting and sub-processing.
- Understand the responsibilities of data controller and data processor in Sub-contracting or Sub-processing.



Responsibilities of Controllers and Processors in Cases of Subcontracting or Sub-processing

Subcontracting, also known as sub-processing, describes a scenario in which a data processor, who is originally hired by a data controller to process personal data on the controller's behalf, subcontracts some or all of the data processing tasks to another party. The original processor is now the supplier or sub-processor in this chain of data handling, and they are responsible for everything



Sub-contracting: is a business practice where one company (the primary contractor or subcontractor) enters into an agreement with another company (the sub-contractor) to perform specific tasks, services, or parts of a project on its behalf. This arrangement allows the primary contractor to delegate certain responsibilities or aspects of a project to another entity while retaining overall control.

Sub-processing: in the context of data protection and privacy regulations, especially under the Nigeria Data Protection Act (NDPR), refers to a situation where a data processor (the primary entity processing personal data) engages another data processor (the sub-processor) to assist in specific data processing activities. Both the data processor and sub-processor must comply with data protection regulations and have contractual agreements specifying their roles and responsibilities.

Consider the following scenario as an example of this idea:

Data Controller: This is the person, business, or group that gathers personal data and decides how and why it will be used. The person in charge of data is responsible for making sure that personal data is handled in a way that follows data security rules and respects the rights of data subjects.

Data Processor: The person in charge of the data can hire a data processor to do certain data processing tasks for them. The controller gives directions to the processor, and the processor must follow those instructions and follow data protection rules.

In some situations, the main data processor (also called the primary processor) may need to hire another person, business, or organisation to do some of the data processing work. This group or person is now the supplier or sub-processor. For the main processor, which in turn handles data for the data controller, the sub-processor works on the data.

Consent and Proof: If a data processor (the main processor) wants to use a subcontractor or sub-processor, they need to get written permission from the data owner first. Usually, this permission is written down in a contract. The person in charge of the data still has control over it and knows about any participation from subcontractors.

Chain of Responsibility: The person who is in charge of the data is mostly responsible for making sure that personal data is handled legally and in line with data protection laws. These people do some of the same tasks as the data worker, though. After that, the data processor is responsible for what the supplier or sub-processor does.

When is a contract needed?

The contract known as the Data Processing Agreement (DPA) contract is needed when a controller uses a processor to process personal data, and whenever a processor employs another processor (a 'sub-processor').

Data Protection Agreements: In these kinds of relationships, data processing agreements are necessary. These agreements must include subcontracting clauses. Each party, including the subcontractor, should know what their duties and responsibilities are in these agreements so that data security standards are met.

Under the NDPR, the following details and provisions must be specified in any data processing contract.

- **Processing Details**

The contract between a controller and a processor must include the following information:

- The subject matter of the processing.
- The duration of the processing.
- What processing will be done;
- The purpose of the processing.
- The type of personal data being handled.
- The categories of data subjects; and
- The obligations and rights of the data controller

▪ **Controller's Instructions**

Also, the contracts should stipulate that the processor can only process personal data as per the controller's written instructions, except when required by law. If legal obligations demand data disclosure, the processor must notify the controller beforehand, unless prohibited by law for public interest reasons.

▪ **Duty of Confidence**

The Contracts should obligate processors to secure confidentiality commitments from those handling personal data (unless legally bound to do so). This extends to the processor's employees, temporary and agency workers, and subcontractors, all of whom must engage in confidentiality agreements with the processor.

▪ **Security Measures**

Processors must adhere to the same security requirements as controllers, this includes implementing appropriate technical and organizational measures such as encryption, pseudonymisation, processing system resilience, and personal data backup.

Data Security: To protect the privacy, accuracy, and availability of personal data, everyone involved, even subcontractors, must take the right data security steps. The original data controller's rules and data security laws must be followed.



3.2.3 In cases of subcontracting and sub-processing, the roles and responsibilities of data controllers include the following.

- The responsibility for guaranteeing the protection of personal data and monitoring compliance with security measures lies with data controllers.

- Controllers are responsible for overseeing and ensuring that data processors comply with data protection legislation by promptly reporting any incidents of personal data breaches to the relevant supervisory body.
- When there is a breach of personal data, data controllers are responsible for supervising and overseeing the procedure of informing the individuals whose data has been compromised.
- Data controllers are responsible for providing access to personal data that is being processed by data processors. They also handle the management of answers to subject access requests made by data subjects.

The end of contract, the data processor:

- Unless required by law, data controllers determine the management of personal data at the contract's completion, specifying whether the data should be wiped or returned.
- Data controllers have the authority to decide how personal data will be managed once a contract ends. They can choose to either delete the data or return it, unless there is a legal obligation to retain it.



In cases of subcontracting and sub-processing, data processors assist data controllers in the following roles.

- Processors shall help controllers in reporting cases of personal data breaches to the appropriate supervisory authority.
- Processors must assist controllers in ensuring the security of personal data.
- In the case of a personal data breach, processors must assist controllers in notifying data subjects.
- Processors must grant controllers access to the data they process and assist them in responding to subject access requests from data subjects.

The end of contract, the data processor:

- Unless required by law, all personal data should be erased or returned at the conclusion of the contract, as determined by the controller.

Others

Consent for Sub-Processors:

- Prior to engaging sub-processors, processors must get written permission from the controller. This consent might be provided in general or in specific cases.
- In circumstances where changes to approved sub-processors are normally permitted, the processor must notify the controller of any changes, giving the controller the opportunity to object if necessary.

Topic 3

Real-life Data Processing Scenarios

Under this topic, the following key areas shall be discussed:

- 3.3.1 Learning Expectations from the Case Study.
- 3.3.2 Real-life examples of data processing
- 3.3.3 Real life scenarios in classifying a data processor and data controller.
- 3.3.4 Questions and Answers

Time Allocated: 15 mins



Real-life Data Processing Scenarios

3.3.1 Learning Objectives

Upon completion of Topic 3 “Responsibilities of Controller and Processors in cases of Sub-contracting and Sub-processing”, participants shall be equipped with the skills to:

- Participants will understand and distinguish the roles of data controller, processor, and subject, clarifying data handling responsibilities.
- Participants will apply their data protection and privacy knowledge to a real-life scenario.
- Participants will learn how data is collected, processed, stored, and protected in a data processing scenario, enhancing their understanding of data processing dynamics.

3.3.2 Scenario (1)

Background: Shop World is a widely recognised e-commerce platform that facilitates transactions between millions of customers and a diverse array of retailers and sellers, enabling the purchase of an extensive variety of products.

The Data Controller is:

Shop World assumes the role of the data controller in the given context. They establish the methods and rationales behind the collection and processing of customer data.

Data Collection: Shop World gathers an extensive range of customer data, encompassing sensitive information (such as location data for delivery purposes) and personal details (including names, addresses, and email addresses).

Processing of Data for Diverse Objectives:

- **Order Processing:** Shop World processes and fulfils orders using customer information to ensure that products are delivered to the correct addresses.

- **Personalization:** Personalization involves the examination of customer shopping patterns and inclinations in order to deliver customised shopping experiences and personalised product suggestions.
- **Marketing:** Customers are sent promotional emails and offers by ShopWorld in accordance with their past purchases and areas of interest.
- **Legal Compliance:** It is the responsibility of ShopWorld to ensure that the handling of customer data adheres to data protection regulations. To achieve this, the company must establish transparent privacy policies and consent mechanisms.

Data Processors:

Shop World relies on several data processors to support its operations:

- **Payment Processing Services:** When customers make purchases, payment processors like PayPal and Stripe handle the financial transactions securely.
- **Data Analytics Software:** Shop World uses data analytics software to gain insights into customer behavior, helping them improve their services and recommendations.
- **Email Marketing Platform:** An email marketing platform assists Shop World in sending promotional emails and newsletters to customers.
- **Third-Party Retailers and Sellers:** Retailers and sellers using the Shop World platform to sell their products may also act as data controllers for their specific customer data, especially when they interact directly with customers.

As a Controller:

- Responsible for informing clients of the intended use of their data and obtaining their consent when required.
- Is accountable for ensuring the protection and security of the customer data that is gathered?
- It is imperative to develop unambiguous policies and processes in order to guarantee adherence to data protection regulations.
- Payment processors, email marketing platforms, and analytics software are examples of data processors.

As a Processor:

- Responsible for managing customer information in adherence to ShopWorld's protocols and security criteria.
- Customer information should not be utilised for any purpose not authorised by Shop World.

Interactions and Discussions 3



3.3.3 Based of the above Real-life scenarios in classifying a data processor and data controller, lets determine the right answer and why (Time Allocated: 15 mins)

Question 1: In the case of a cloud provider used to store student information for a university, is the cloud provider a data controller, data processor, or neither?

Question 2: When an accountancy firm prepares the accounts for a company, what is the role of the accountancy firm in terms of data processing, and is it acting as a data controller or data processor?

Question 3: When a company is used for processing credit card payments made when customers make online purchases, how should the company's role in processing payment data be classified, and is it a data controller or data processor?

QUESTION



Tips for Trainer

- Clearly communicate the learning expectations at the outset, outlining the knowledge participants should gain from the session.
- Provide a clear and concise introduction to the roles of data controllers and processors, ensuring participants understand the distinctions and responsibilities.
- Explore in-depth the specific roles and responsibilities of both data controllers and data processors, emphasizing their individual obligations.
- Clearly define the obligations associated with being a data controller or data processor, ensuring participants understand the legal and ethical considerations.
- Explore the intricacies of the relationship between data controllers and data processors, emphasizing effective communication and collaboration.
- Clearly define sub-contracting and sub-processing, providing participants with a comprehensive understanding of these concepts.
- Articulate the roles of data controllers and processors when sub-contracting or sub-processing occurs, emphasizing compliance and accountability.
- Delve into the specific responsibilities of data controllers and processors in cases of sub-contracting or sub-processing, covering legal and operational aspects.
- Integrate real-life examples of data processing scenarios to illustrate theoretical concepts, facilitating practical understanding among participants.
- Use case studies to demonstrate real-life scenarios of classifying data processors and controllers, encouraging participants to apply theoretical knowledge.
- Foster active engagement through an interactive discussion of case studies, allowing participants to share insights and perspectives.
- Connect lessons learned from case studies to real-world applications, emphasizing the relevance and applicability of the discussed principles.
- Allocate dedicated time for questions and answers, allowing participants to seek clarification on complex concepts related to data processing.
- Discuss common challenges faced by data processors and controllers, providing practical strategies for overcoming these challenges.
- Utilize interactive scenarios to reinforce learning, allowing participants to apply their knowledge in simulated data processing situations.

SECTION 4

Managing Data Security Incidents and Breaches

Topic 1

Strategies for Identifying and Responding to Data Security Incidents

Under this topic, the following key areas shall be discussed:

- 4.1.1 Learning Outcomes
- 4.1.2 What is a Data Security Incident?
- 4.1.3 Common Security Incidents
- 4.1.4 Strategies for Identifying and Responding to Data Security

Time Allocated: 15 mins



Strategies for Identifying and Responding to Data Security Incidents

4.1.1 Learning Objectives

Upon completion of Topic 1 “Strategies for identifying and Responding to Data Security Incident”, participants shall be equipped with the skills to:

- Educate DPOs with the essential knowledge and expertise to promptly and efficiently address data security incidents and breaches.
- Equip Data Protection Officers (DPOs) to assume leadership roles within incident response teams, thereby mitigating the adverse effects of security breaches on the organisation.





Strategies for Identifying and Responding to Data Security Incidents

4.1.2 What are Security Incidents?

Security incidents are events or occurrences that pose a threat to the confidentiality, integrity, or availability of an organization's information and resources. These incidents can include a wide range of activities and situations that compromise the security of an organization's assets, including data, systems, networks, and physical facilities. Security incidents can be intentional, such as cyberattacks and data breaches, or unintentional, such as system failures or employee errors.



What is a Data Security Breach?

Data incident is any event or situation that could jeopardize the security of personal or sensitive data in the context of data protection. Unauthorized access, data breaches, data loss, or any other event that jeopardizes the confidentiality, integrity, or availability of data are examples of such incidents. To ensure the privacy and security of individuals' data, effective data protection measures are in place to prevent and respond to such incidents.



4.1.3 Common Examples of Security Incidents

- **Cyberattacks:** These can involve activities like hacking, malware infections, distributed denial of service (DDoS) attacks, and phishing attempts, with the aim of gaining unauthorized access to systems or stealing sensitive data.
- **Data breaches:** This includes unauthorized access or disclosure of sensitive or confidential information, which can result in data leaks, identity theft, or reputational damage.

- **Insider threats:** These are actions by individuals within an organization, such as employees or contractors, who misuse their access or privileges to harm the organization's security, often unintentionally or with malicious intent.
- **Physical security incidents:** This includes events like break-ins, theft, vandalism, or natural disasters that can impact an organization's physical infrastructure and assets.
- **Human errors:** This incident is as a result of mistakes made by employees or users, such as accidentally deleting critical data, misconfiguring systems, or sending sensitive information to the wrong recipient.
- **Compliance violations:** This includes failing to adhere to legal or regulatory requirements related to security and data protection, which can result in legal penalties and fines.
- **Security policy violations:** Breaking internal security policies, whether knowingly or unknowingly, can lead to incidents that compromise security.
- **Malicious insiders:** Employees or individuals with privileged access who intentionally sabotage or compromise an organization's security for personal gain or vendetta.
- **Phishing Attacks:** These are emails or messages that are meant to trick people into giving up sensitive information, like login credentials, which can lead to data breaches or unauthorized access.
- **Malware Infections:** Bad software can weaken data security, letting hackers steal private data, stop operations, or change data in other ways.
- **Social engineering** attacks are a type of manipulation that uses the way people think and feel to get them to reveal private information or let someone in without permission



Strategies for Identifying and Responding to Data Security Incidents

4.1.4 Identifying Data Security Incidents

Identifying and responding to data security incidents effectively is crucial for protecting an organization's sensitive information and minimizing potential damage. Here are strategies for both identifying and responding to data security incidents:

STRATEGIES



Here are strategies to help organizations identify and respond to data and security incidents effectively:

- **Implement Privacy and Security Monitoring:** Employ Privacy and security monitoring tools and techniques to actively monitor network traffic, system logs, and user activities for signs of suspicious or anomalous behavior. This can include intrusion detection systems, intrusion prevention systems, Data Loss Prevention solution (DLP), and security information and event management (SIEM) solutions.
- **Use Anomaly Detection:** Utilize anomaly detection algorithms to identify deviations from normal system behaviour. These algorithms can help detect unusual patterns or activities that may indicate a security incident.
- **Regular Vulnerability Scanning:** Conduct regular vulnerability assessments and scans to identify weaknesses in systems and applications that could be exploited by attackers.

- **User Training and Awareness:** Train employees and users to recognize potential security threats, including phishing emails, social engineering attempts, and other common attack vectors.
- **Threat Intelligence Sharing:** Stay informed about the latest threats and vulnerabilities by participating in threat intelligence sharing communities and subscribing to threat feeds. This information can help you proactively identify emerging security threats.
- **Incident Reporting Mechanisms:** Establish clear incident reporting mechanisms, such as a designated email address or hotline, where employees and users can report suspicious activities or incidents they encounter.
- **Regular Audits and Reviews:** Conduct periodic security audits and reviews of systems and policies to identify potential weaknesses or compliance violations.

Responding to Data Security Incidents:

- **Have an Incident Response Plan:** Develop and maintain a comprehensive incident response plan that outlines the steps to take when a security incident is detected. The plan should include roles and responsibilities, communication procedures, and actions to be taken during each phase of the incident response.
- **Contain the Incident:** Isolate affected systems, networks, or data to prevent the incident from spreading. This may involve disconnecting compromised devices from the network or blocking malicious traffic.
- **Notify Relevant Parties and Authorities:** Ensure that the appropriate personnel, such as IT staff, legal teams, and senior management, are informed about the incident. Depending on the nature of the incident, you may also need to notify external parties, like law enforcement or regulatory bodies. Data breaches must be reported to the NDPC within 72 hours and affected data subjects must be informed promptly.

- **Preserve Evidence:** Document and preserve evidence related to the incident, which may be necessary for investigations, legal proceedings, or regulatory compliance.
- **Investigate the Incident:** Conduct a thorough investigation to understand the scope, impact, and root cause of the incident. This may involve examining logs, conducting forensics analysis, and interviewing relevant personnel.
- **Mitigate the Incident:** Develop and implement strategies to mitigate the incident's impact. This can include patching vulnerabilities, removing malware, or implementing additional security controls.
- **Communication:** Maintain open and transparent communication with stakeholders, both within the organization and externally, as needed. Keep affected parties informed about the incident's status, potential risks, and recovery efforts.
- **Legal and Regulatory Compliance:** Ensure that your response is in accordance with relevant laws and regulations, especially if the incident involves sensitive data or personal information.
- **Lessons Learned:** After resolving the incident, conduct a post-incident review to identify areas for improvement in your incident response process and security controls.
- **Documentation:** Document all aspects of the incident response, from initial detection to resolution, for future reference and to help improve incident response procedures.
- **Continuous Improvement:** Use the lessons learned from the incident to refine your organization's security posture and incident response plan to better prepare for future incidents.

Topic 2

Best Practices for Mitigating the impact of Data Breaches and Ensuring Compliance

Under this topic, the following key areas shall be discussed:

- 4.2.1 Learning Expectations
- 4.2.2 Introduction to Data Breaches
- 4.2.3 Causes and impact of Data Breach
- 4.2.4 Best Practices for mitigating Data Breaches and Ensuring
- 4.2.5 Case Study Illustrations

Time Allocated: 10 mins



Best Practices for Mitigating the impact of Data Breaches and Ensuring Compliance

4.2.1 Learning Objectives

Upon completion of Topic 2 “Managing Data Security Incident and Breaches”, participants shall be equipped with the skills to:

- Enabling DPOs to respond effectively to incidents and breaches, thereby safeguarding the organization's reputation.
- Enhancing the professional capabilities of DPOs, making them valuable assets to their organizations



The objective of the "Managing Data Security Incidents and Breaches" training session for Data Protection Officers (DPOs) is to provide Data Protection Officers (DPOs) with a thorough comprehension of the definition of a data security incident and its distinction from a data breach. This includes identifying common examples of incidents and their potential implications.



Best Practices for Mitigating the impact of Data Breaches and Ensuring Compliance

4.2.2 Introduction to Data Breach

A data breach is a cybersecurity incident in which unauthorized individuals or entities gain access to sensitive, confidential, or protected data, and in some cases, compromise, steal, or misuse that information. Data breaches can occur in various forms and can have severe consequences for individuals, organizations, and even society as a whole.



The difference between data security incident and a data breach

Data Security Incident:

A data security incident is any event or occurrence that has the potential to jeopardize an organization's data or information systems' confidentiality, integrity, or availability. This encompasses a wide range of activities or circumstances that may or may not result in a data breach. Intentional (e.g., cyberattacks) or unintentional (e.g., system failures, employee errors) data security incidents can occur.

Not every data security incident results in a data breach. For example, if a security system detects and prevents a cyberattack attempt before data is accessed or stolen, the incident is still classified as a security incident rather than a breach.

Data Breach: Data breach is a type of data security incident that involves the unauthorised access, acquisition, disclosure, or release of sensitive or confidential data. It denotes a security incident that resulted in a confirmed data compromise. And they occur as a result of a variety of factors, such as cyberattacks, insider threats, hacking, or even unintentional exposure.

Data breaches can involve a wide range of data types, including personal information (e.g., names, addresses, Social Security numbers), financial data (e.g., credit card numbers, bank account details), medical records, intellectual property, and more. The breaches may occur through unauthorized access to digital systems or physical theft of data-bearing devices.



4.2.3 Common causes of data breaches include:

- **Cyberattacks:** Malicious actors use various techniques, such as hacking, phishing, malware, and social engineering, to gain unauthorized access to computer systems and networks.
- **Insider Threats:** Employees, contractors, or other individuals with inside knowledge can intentionally or accidentally compromise data security.
- **Lost or Stolen Devices:** Laptops, smartphones, external hard drives, or other devices containing sensitive data can be lost or stolen, putting the information at risk.
- **Weak Security Practices:** Inadequate security measures, including weak passwords, unpatched software, and insufficient encryption, can make systems vulnerable to breaches.



4.2.4 Impacts of Data Breaches

Data breaches can have significant consequences, including:

- **Financial Loss:** Organizations often face substantial financial losses due to data breach response costs, legal penalties, and reputational damage.
- **Legal and Regulatory Consequences:** Data breaches can result in legal actions and regulatory fines, especially if they involve violations of data protection laws.
- **Reputational Damage:** A breach can erode trust and reputation with customers, partners, and the public.
- **Identity Theft and Fraud:** Stolen personal information can lead to identity theft and financial fraud for individuals affected by the breach.
- **Business Disruption:** Data breaches can disrupt normal business operations, causing downtime and loss of productivity.
- **Data Privacy Violations:** Breaches may infringe upon individuals' rights to data privacy and trigger investigations and lawsuits.



2023 Top World statistics on data breaches

- Number of incidents in September 2023: 71
- Number of breached records in September 2023: 3,808,687,191
- Number of incidents in 2023: 838
- Number of breached records in 2023: 4,500,775,104
- Biggest data breach of 2023 so far: DarkBeam (3.8 billion breached records)
- Biggest data breach in the UK: Electoral Commission (40 million breached records)

Here are some of the significant data breaches and cyberattacks that occurred in 2023

- **DarkBeam (September 2023):**

DarkBeam, a company specializing in digital risk protection, inadvertently made 3.8 billion records accessible to the public as a result of a misconfigured Elasticsearch and Kibana interface. Although a majority of the compromised data originated from past security breaches, the vast amount of information possessed by DarkBeam presented a significant risk for conducting phishing campaigns.

- **Report from the UK Electoral Commission (August 2023):**

The UK Electoral Commission experienced a sophisticated cyber-attack, during which malicious actors successfully breached the UK's electoral registers, impacting approximately 40 million individuals. The assailants obtained unauthorised access to the personal information of voters, including their names, addresses, and voting records.

- **Indonesian Immigration Directorate General (July 2023):**

An unauthorised individual successfully infiltrated the Indonesian Immigration Directorate General's system, resulting in the disclosure of passport information belonging to over 34 million Indonesian citizens.

- **Luxottica (May 2023):**

Luxottica, a prominent global eyewear corporation, suffered a substantial data breach, resulting in the exposure of personal information belonging to 74.4 million distinct email addresses and 2.6 million unique domain email addresses.



Best Practices for Mitigating the impact of Data Breaches and Ensuring Compliance

4.2.4 Introduction to Data Breach

Mitigating the impact of data breaches and ensuring compliance is crucial for organizations to protect sensitive information and maintain trust with customers, partners, and regulatory authorities.



Some best practices to help mitigate the impact of a data breach in an organization are listed below.

Data Classification:

- Classify data based on its sensitivity, ensuring that critical data is more protected.
- Apply access controls and encryption to data based on its classification.

Regular Risk Assessments:

- Conduct ongoing risk assessments to identify potential vulnerabilities and threats.
- Use risk assessment results to prioritize security investments and measures.

Access Control:

- Implement the principle of least privilege to limit access to data.
- Use strong authentication methods, such as multi-factor authentication (MFA), to enhance access security.

Encryption:

- Encrypt data at rest and in transit, using industry-standard encryption algorithms.
- Ensure that encryption keys are securely managed and stored separately from the data.

Employee Training and Awareness:

- Train employees on security best practices and the risks of data breaches.
- Promote a culture of security awareness, encouraging employees to report suspicious activities.

Incident Response Plan:

- Develop a well-defined incident response plan that outlines steps to take in the event of a breach.
- Regularly test and update the plan, involving key stakeholders.

Data Backup and Recovery:

- Implement regular data backup and recovery procedures to minimize data loss during a breach.
- Store backups in secure, isolated locations.

Data Retention and Destruction:

- Implement a data retention policy to avoid keeping data longer than necessary.
- Properly dispose of data, including securely erasing or shredding physical media.

Incident Reporting:

- Promptly report data breaches to relevant authorities, as required by applicable regulations.
- Notify affected individuals when necessary and provide guidance on protecting their information.

Monitoring and Logging:

- Implement robust monitoring and logging systems to detect and investigate suspicious activities.
- Retain logs securely and review them regularly.

Legal Counsel:

- Engage legal counsel experienced in data breach and compliance issues to guide your response and legal obligations

Interactions and Discussions 4



Case Study

Time Allocated: 15 mins

In understanding the challenges of dealing with data breaches and the importance of being well-prepared to respond effectively. Let's look at this scenario

Background:

AMI Healthcare is a large hospital network that handles sensitive patient data. The organization is committed to maintaining the privacy and security of patient information. However, despite their best efforts, they experienced a significant data breach.

Scenario: In late 2022, AMI Healthcare discovered that a data breach had occurred within their system. The breach was first detected when the IT department noticed unusual network activity and unauthorized access to patient records. The breach impacted both electronic health records (EHR) and personal patient information.

Key Details:

- The breach affected 100,000 patient records.
- Data exposed included names, addresses, social security numbers, medical diagnoses, and treatment histories.

- It was later revealed that the breach resulted from a phishing attack on an employee that led to unauthorized access.

Discussion Points:

1. Incident Discovery:

When and how was the breach discovered?

What were the initial signs or red flags that indicated a breach?

2. Immediate Response

What steps should AMI Healthcare take immediately after discovering the breach?

Who should be involved in the initial response?

What are the legal and regulatory obligations in this situation?

3. Investigating the Breach:

How should the organization investigate the breach to determine its scope and the extent of the data exposed?

4. Data Protection Measures

What data protection measures should have been in place to prevent this breach?

How could employee awareness and training have played a role in preventing the phishing attack?

5. Legal and Regulatory Compliance

What are the legal and regulatory requirements for reporting the breach to authorities and affected patients and what potential fines or penalties could AMI Healthcare face?

6. Communication and PR

How should AMI Healthcare communicate the breach to affected patients?

What strategies can the organization use to manage its public relations and reputation?

7. Preventing Future Breaches

What measures should AMI Healthcare implement to prevent similar incidents in the future?

How can employee training and awareness be improved?

8. Lessons Learned:

What lessons can AMI Healthcare and other organizations learn from this breach?

How can this case study inform best practices for data breach prevention and response?





Tips for Trainer

- Clearly articulate the learning outcomes at the beginning, providing participants with a roadmap for what they will gain from the session.
- Provide a clear definition of data security incidents, ensuring participants understand the broad spectrum of incidents that may occur.
- Discuss common security incidents to familiarize participants with various scenarios, fostering a comprehensive understanding.
- Elaborate on effective strategies for identifying and responding to data security incidents, emphasizing the importance of a proactive approach.
- Clearly communicate the learning expectations for the section on data breaches, preparing participants for the in-depth exploration of this critical topic.
- Provide insights into the causes and impact of data breaches, ensuring participants grasp the severity and implications of such incidents.
- Discuss best practices for mitigating the impact of data breaches and ensuring compliance, focusing on proactive measures and response strategies.
- Integrate case study illustrations to demonstrate real-world scenarios, allowing participants to apply theoretical knowledge to practical situations.
- Clearly articulate the distinction between data security incidents and data breaches, ensuring participants understand the nuances between these terms.
- Discuss significant data breaches and cyberattacks that occurred in 2023, offering insights into real-world examples to enhance understanding.
- Emphasize the role of compliance in mitigating data breaches, highlighting the intersection of legal requirements and security practices.
- Foster an interactive environment for discussions, encouraging participants to share experiences and insights related to managing data security incidents.
- Integrate best practices into the discussion, emphasizing the importance of adopting a proactive and preventive approach to data security.
- Discuss emerging threats in the cybersecurity landscape, preparing participants for evolving challenges in managing data security incidents.
- Allocate dedicated time for questions and answers, allowing participants to seek clarification on complex aspects of managing data security incidents and breaches.

SECTION 5

Overview of the Nigerian Data Protection Act

Topic 1

Legal Obligations of Data Controllers, Processors and Data Protection Officers.

Under this topic, the following key areas shall be discussed:

- Learning Expectations
- Overview of the Nigerian Data Protection Act (2023)
- Legal Foundations for Data Processing
- Data Protection Impact Assessments (DPIAs)

This training topic covers crucial aspects of data protection in Nigeria. We will begin by outlining what you can expect to gain from this training and ensure that you are well-prepared for the journey ahead. The Nigerian Data Protection Act will be briefly introduced to provide context for the rest of the training. We will focus on the legal principles that govern data processing, with particular emphasis on the lawful bases that permit data processing in accordance with the law. Additionally, we will explore practical procedures such as maintaining Data Processing Records and conducting Data Protection Impact Assessments (DPIAs), which are essential for ensuring data protection compliance and security.

Time Allowed: 20 minutes



Legal Obligations and Applicable to Data Controllers, Processors and Data Protection Officers.

Learning Objectives

Upon completion of Topic 1 “Legal Requirements and Implications for Data Controllers, Processors and Data Protection Officers (DPOs)”, participants shall be equipped with the skills to:



- Identify the key components and provisions of the Nigerian Data Protection Act.
- Recognize the legal obligations and consequences for non-compliance with the NDPA
- Explain the legal foundations that govern data processing and the various lawful bases that permit data processing according to the NDPA.
- Identify the key components and provisions of the NDPA that relate to DPIA.
- Recognize when and how to conduct a DPIA for your data processing activities.



Nigeria Data Protection Act 2023

Overview of the Nigerian Data Protection Act 2023

The Nigeria Data Protection Act 2023 (NDPA) is a law that provides a legal framework for data protection and privacy in Nigeria. It was signed into law by **President Bola Ahmed Tinubu on 12 June 2023.**



What You Need to Know About the Data Protection Act!

The NDPA establishes the Nigeria Data Protection Commission (NDPC) as the independent data protection authority for Nigeria, and regulator in Nigeria. The NDPC is responsible for enforcing the provisions of the NDPA and the administration of all data protection matters in Nigeria.

The Nigerian Data Protection Act (NDPA) applies to any individual or organization, regardless of whether it is in the public or private sector, and regardless of location, as long as the personal data being processed relates to a data subject in Nigeria.

The NDPA (National Data Protection Act) lays out eight data protection principles that Data Controllers and Processors must adhere to. These principles are:

- lawfulness, fairness, and transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation

- integrity and confidentiality
- accountability and duty of care

The Nigerian Data Protection Act (NDPA) places specific responsibilities on Data Controllers and Processors. These include acquiring valid consent from data subjects, implementing suitable technical and organizational measures to safeguard personal data, reporting data breaches to the NDPC and data subjects, carrying out data protection impact assessments, designating data protection officers, and registering with the NDPC.

The Act introduces legitimate interest as an additional legal basis for processing personal data, in addition to consent, contractual obligation, legal obligation, vital interest, and public interest.

The Act also classifies personal data into two categories: general personal data and sensitive personal data. The Act defines sensitive personal data as personal data that reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life of a data subject. The Act requires a higher level of protection for such data and imposes stricter conditions for its processing.

Legal Obligations of the Nigerian Data Protection Act!

The Nigerian Data Protection Act (NDPA) places several obligations on Data Controllers and Processors. These include:

- Acquiring explicit consent from individuals before handling their personal data, always ask people for permission before you use their personal data, unless there's a good reason not to.
- Providing data subjects with clear and concise details about the handling of their personal data, you tell them why you're using their data, who else might see it, how long you'll keep it, and how they can ask questions or make requests.
- Enforcing suitable technical and organizational measures - Think of personal data as a valuable treasure. You need to keep it safe and secure. If something goes wrong and there's

a data breach, you must report it to the Data Protection Commission and tell the people affected within 72 hours.

- Adhering to the fundamental data protection principles, which include acting lawfully, fairly, and transparently, limiting data use to its intended purpose, minimizing data collection, maintaining accuracy, storing data for appropriate durations, and being accountable for data processing activities

- Recognizing and respecting the rights of individuals - Imagine you're borrowing someone's favorite book. They might want it back, or they may want to make some notes in it. It's the same with personal data. People have the right to access it, correct it, delete it, or ask you to stop using it.

- Registering with the NDPC and designating a Data Protection Officer (DPO) if you handle the personal data of over 1,000 individuals annually or sensitive personal data of more than 250 individuals annually.

- Conducting a Data Protection Impact Assessment (DPIA) before engaging in any data processing activities that pose significant risks. It's like a safety check.

- Seeking authorization from the NDPC prior to transferring personal data outside Nigeria, except when the destination country or region ensures an adequate level of data protection.



Consequences of Non-compliance of the Nigerian Data Protection Act!

Breaking data protection laws can lead to penalties as per the NDPA rules. For larger organizations like major companies, a fine of 2% of their yearly earnings or 10 million Naira, whichever is more, may be imposed, while smaller organizations may have to pay 1% of their yearly earnings or 2 million Naira, whichever is more. The fine amount depends on the size of the organization.

Data subjects who have suffered damages due to mishandling of their personal data may request civil liability and compensation.

How Do You Come In As A Data Protection Officer?

The Data Protection Officer (DPO) plays a crucial role in making sure that Data Controllers and Processors follow the rules. Their job involves watching, guiding, and reporting on how well everyone sticks to data protection laws like the NDPA. Think of the Data Protection Officer (DPO) as the data guardian.

The connection between the DPO and the data controller/processor is a bit like having a coach who guides you through a game. The DPO helps these teams understand what they need to do to follow the rules and ensures they're doing things the right way. If there are problems or rule violations, the DPO informs the team and suggests ways to fix things. Importantly, the DPO reports directly to the top management of the company, but they work independently when it comes to data protection tasks and don't take instructions from the higher-ups, like a trusted advisor.



Actions to be taken by the DPO to ensure Data Controllers & Processors are meeting Obligations:

- **Education and Awareness:** The DPO is responsible for educating Data Controllers and Processors about their legal obligations under the NDPA.
- **Policy Development and Implementation:** The DPO actively participates in the development and implementation of data protection policies and procedures within the organization.
- **Compliance Monitoring:** The DPO monitors data processing activities to ensure compliance with the NDPA.
- **Advice and Guidance:** The DPO acts as a trusted advisor to Data Controllers and Processors, providing guidance on how to process data in compliance with the NDPA. They offer solutions and best practices to address specific challenges or issues related to data protection.
- **Data Subject Rights Protection:** The DPO ensures that data subjects' rights are protected. They guide Data Controllers and Processors in responding to data subject requests, such as access, rectification, or erasure, and assist in ensuring that these requests are handled within the NDPA's timelines.
- **Vendor and Third-Party Management:** The DPO assesses the data protection practices of third-party Data Processors or vendors that the organization engages with. They ensure that appropriate data protection agreements are in place and that these third parties comply with the NDPA.
- **Record of Processing Activities (RoPA):** The DPO maintains a comprehensive RoPA that documents all data processing activities within the organization. This record serves as a fundamental tool for transparency, accountability, and compliance with the NDPA.



Legal Foundations for Data Processing

The lawful basis for processing personal data are listed in Section 8 of the NDPA 2023. Data Protection Officers (DPOs) are responsible for ensuring that Data Controllers and Data Processors comply with the Act and protect the rights and privacy of data subjects.



Lawful Basis for Processing Data According to The Data Protection Act!

The NDPA establishes the Nigeria Data Protection Commission (NDPC) as the primary data protection authority and regulator in Nigeria.

- **Consent:** Imagine consent as a green light given by the data subject. It means the individual has explicitly given their permission for you to process their personal data. Consent can be for one or more specific purposes. It's like asking for someone's permission before taking any action with their data.
- **Contractual Obligation:** You process personal data because it's required to fulfil a contract with the data subject. It could also involve taking steps before entering into a contract, such as collecting data to prepare for a business deal. It's like having a contract that outlines the rules, and you follow those rules.

- **Legal Obligation:** This is all about following the law. You process personal data because there's a legal duty imposed on you to do so. It's like obeying traffic laws because the government says you must. It's not a choice; it's a must-do.
- **Vital Interest:** When someone's life or health is on the line, you can process their data to protect them. It's like calling an ambulance when you see someone in urgent need. You're doing it to save a life, and that's the priority.
- **Public Interest:** Sometimes, processing personal data is necessary for the greater good. It means you're doing something that benefits the public or is part of an official duty. It's like a firefighter rescuing people from a burning building – it's for the safety and well-being of everyone.
- **Legitimate Interest:** Imagine this as a balancing act. You can process personal data for your own or a third party's legitimate interests, but only if those interests don't outweigh the rights and freedoms of the data subject. It's like considering the pros and cons – if it's necessary and fair, you can proceed.



How to Determine Which Lawful Basis to Use for Your Data Processing Activity

Selecting the appropriate lawful basis for your data processing activity is crucial to ensure compliance with data protection regulations. Here's a step-by-step guide to help you determine which lawful basis to use:

- **Identify the Purpose:** Start by clearly defining the purpose of the data processing activity. First, be clear about why you need the data. Is it for a contract, a legal rule, consent, because it's important for someone's safety, a public job, or because you have a good reason? Make sure your purpose is clear.
- **Consider Consent:** If you can obtain the individual's explicit and informed consent for the processing activity, this is often the easiest and safest lawful basis to use. Consent should be freely given, easily withdrawable, and well-documented.

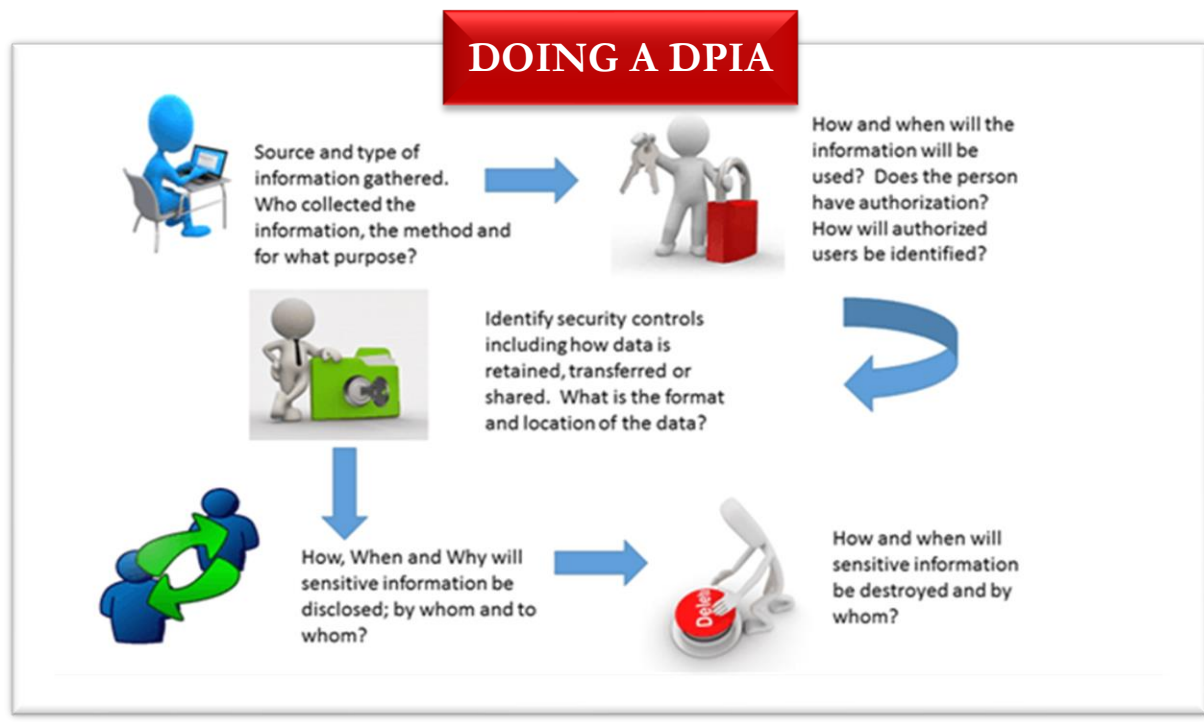
- **Contractual Obligation:** If processing is necessary to fulfil a contract with the data subject or to take pre-contractual steps at their request, then the lawful basis is a contractual obligation.
- **Legal Obligation:** When processing is required to comply with a legal obligation, such as tax reporting or law enforcement, this is the appropriate lawful basis.
- **Vital Interests:** If processing is necessary to protect someone's life or physical integrity, the lawful basis is vital interests. This is often applicable in emergency situations when it's about protecting someone's life or health and you can't get their permission or consent.
- **Legitimate Interests:** If you can show a legitimate interest in processing the data, and this interest is not overridden by the rights and interests of the data subject, you can use legitimate interests as the lawful basis. Conduct a legitimate interest assessment to weigh the interests and ensure they are balanced.

If you are handling sensitive information such as health, racial or ethnic origin, or religious beliefs, you may need to identify an additional lawful basis under the NDPA. It's important to keep records of your decision on the chosen lawful basis and inform data subjects about the lawful basis for processing their data in your privacy notices. It's also crucial to ensure that they understand why and how their data is being used.



Data Protection Impact Assessment (DPIA)

One of the ways to ensure compliance with the Nigeria Data Protection Act (NDPA), is to conduct a Data Protection Impact Assessment (DPIA). A DPIA is a process to help you identify and minimise the data protection risks of a project or plan involving personal data.



According to the NDPA, a DPIA should be conducted before engaging in any data processing activity that is likely to result in a high risk to the rights and freedoms of data subjects. The NDPA does not provide a specific list of cases that require a DPIA, but it refers to the criteria and examples provided by the GDPR. Based on these sources, some of the cases that may require a DPIA are:

- Large-scale processing of personal data that affects a large number of individuals or involves sensitive or detailed information.
- Automated decision-making or profiling that produces legal or significant effects on individuals, such as credit scoring, online behaviour analysis, or health diagnosis.
- Processing of special category data or criminal offence data
- Processing that involves new technologies or innovative methods that may pose unknown or unforeseen risks, such as artificial intelligence, blockchain, facial recognition, or the Internet of things.

- Processing that involves tracking or monitoring of individuals' location or behaviour, such as CCTV, geolocation, cookies, or online advertising.
- Processing that involves combining, comparing, or matching data from multiple sources or datasets.
- Processing that involves vulnerable individuals or groups, such as children, elderly people, people with disabilities, or refugees.
- Processing that may affect individuals' physical or mental health, safety, reputation, or financial situation.

How to Conduct a DPIA?





To conduct a DPIA, you need to follow a systematic and comprehensive approach that covers the following steps:

- **Identify the need for a DPIA:** You should screen your data processing activities and determine whether they are likely to result in a high risk to individuals. You can use the criteria and examples provided by the NDPA or the NDPC to help you identify the need for a DPIA.
- **Describe the Data Processing:** You should provide a clear and detailed description of the data processing activities and their purposes.
- **Assess the Risks:** You should assess the potential impact of the data processing on the rights and freedoms of individuals, and identify any risks or threats that may arise from it. You should consider both the likelihood and severity of harm that may occur, such as physical or mental injury, financial loss, identity theft, discrimination, reputational damage, etc.
- **Identify and Implement Measures:** You should identify and implement measures to address the risks and mitigate their impact.
- **Consult with the NDPC and/or data subjects:** You should consult with the NDPC and/or data subjects if the DPIA indicates that the processing would result in a high risk in the absence of measures taken by you to mitigate the risk, or if you are unsure whether the measures are sufficient or effective

Topic 2

Understanding the Role of the Nigerian Data Protection Commission (NDPC)

Under this topic, the following key areas shall be discussed:

-  Learning Objectives
-  Statutory Responsibilities and Legal Authority of the NDPC.
-  Legal Foundations for Data Processing
-  Mechanisms Used by NDPC to Ensure Compliance

This training topic addresses vital aspects of data protection in Nigeria, beginning with an introduction of the Nigerian Data Protection Act to establish context, followed by an exploration of legal principles governing data processing, with a focus on lawful bases; and practical procedures, including maintaining Data Processing Records and conducting Data Protection Impact Assessments (DPIAs) essential for data protection compliance and security.

Time Allowed: 15 minutes



Understanding the Role of the Nigerian Data Protection Commission

Learning Objectives

Upon completion of Topic 2 “Understanding the Nigerian Data Protection Commission (NDPC)”, participants shall be equipped with the skills to:

- Gain a comprehensive understanding of the Nigerian Data Protection Act, its key provisions, and its relevance in data protection.
- Understand the importance of data protection compliance, accountability, and the consequences of non-compliance in the Nigerian regulatory context.





The Role of the Nigerian Data Protection Commission (NDPC)

The primary role of the Nigerian Data Protection Commission (NDPC) is to serve as the central regulatory authority responsible for supervising, implementing, and enforcing the provisions of the Nigeria Data Protection Act (NDPA) 2023, along with addressing various matters about data protection within the Nigerian context.



There is no difference between what the Nigerian Data Protection Bureau (NDPB) did and what the NDPC is doing now, because they are the same entity. The NDPB was renamed as the NDPC in 2023, following the enactment of the Nigeria Data Protection Act (NDPA) 2023 by the National Assembly.

The NDPC has a stronger legal mandate and backing than the NDPB because the NDPA 2023 is a primary legislation that was passed by the National Assembly and assented to by the President of Nigeria, while the NDPB was established by an executive order of the Federal Government. The NDPA 2023 provides a comprehensive legal framework for data protection in Nigeria and empowers the NDPC as the main supervisory and regulatory authority for data protection in Nigeria. The NDPA 2023 also repeals and replaces the Nigeria Data Protection Regulation (NDPR) 2019, which was a subsidiary legislation issued by the National Information Technology Development Agency (NITDA) without any statutory backing.



Statutory Responsibilities and Legal Authority of the NDPC.

▪ **Regulatory Oversight:**

The NDPC is responsible for overseeing and authorizing organizations that provide data protection compliance services. This includes services like data auditing, training, and consultancy.

▪ **Enforcement and Compliance:**

One of the core functions of the NDPC is to enforce compliance with the Nigerian Data Protection Act (NDPA). They monitor Data Controllers and Processors to ensure they follow the NDPA and its associated regulations. They're like data detectives – checking up on Data Controllers and Processors to ensure they're playing by the NDPA and its rules. If someone's not following the rules, the NDPC can hand out penalties. They're also there to help out data subjects, Controllers, and Processors with advice and support to make sure everyone's rights are protected.

▪ **Advocacy and Breach Handling:**

Beyond enforcement, the NDPC plays a pivotal role in advocating for data protection awareness and education. They engage with the public and stakeholders to raise awareness and understanding of data protection principles. The NDPC is a point of contact for individuals who have concerns or complaints about the handling of their personal data. In case of data breaches, they require Data Controllers and Processors to report incidents promptly and ensure that affected data subjects are notified within 72 hours.

▪ **Education and Collaboration:**

To promote best practices and standards, the NDPC conducts research and studies on data protection issues and trends. Their findings are shared in reports and recommendations. The NDPC also hosts workshops, seminars, conferences, and other events to disseminate knowledge about data protection. Importantly, they collaborate with national and international data protection authorities and organizations to share experiences and align policies and regulations.

- **Investigative and Sanctioning Authority:**

The NDPC holds the authority to conduct investigations into any suspected or alleged violations of the NDPA or its associated regulations by individuals or entities. If there's a suspicion that someone's not playing by the NDPA rules, the NDPC can step in and investigate. They'll gather info and evidence and, depending on what they find, they can give out warnings, and instructions, or even put limits on things, or in extreme cases, stop data processing altogether.

- **Regulation of International Data Transfers:**

The NDPC takes charge of regulating the international transfer of personal data from Nigeria to other countries or organizations. Their role is to ensure that the destination country or region provides an adequate level of data protection. The NDPC can authorize such transfers if proper safeguards, such as binding corporate rules, standard contractual clauses, or codes of conduct, are in place. Conversely, they have the authority to prohibit transfers if there is a lack of adequate protection or a risk to the rights and freedoms of data subjects.

Mechanisms and Procedures Used by The NDPC To Ensure Organizations Comply with Data Protection Laws

The NDPC has various mechanisms and procedures to ensure that organizations comply with data protection laws, such as:

- **Registration:** The NDPC requires all organizations that process the personal data of Nigerian residents to register with the Commission and submit a data protection compliance audit report annually.
- **Supervision:** The NDPC has the power to monitor and inspect the activities of Data Controllers and Processors, and to request access to any information, document, or equipment relating to data processing. The NDPC can also conduct audits, investigations, or inquiries into any suspected breach or violation of data protection or regulations.
- **Enforcement:** The NDPC has the authority to impose administrative sanctions or penalties for any non-compliance or infringement of data protection laws or regulations. The sanctions or penalties can include warnings, reprimands, orders to cease or rectify the

violation, fines, suspension or revocation of registration, or referral to law enforcement agencies for criminal prosecution. The NDPC can also issue guidelines, codes of conduct, or best practices for data protection compliance.

- **Education:** The NDPC has the responsibility to promote awareness and education on data protection issues among the public and stakeholders. The NDPC can organize workshops, seminars, conferences, or campaigns to disseminate information and guidance on data protection rights and obligations.

Interactions and Discussions



Case Study 1

Data subjects who are customers of XYZ Bank, a prominent financial institution in Nigeria, report complaints directly to the Nigerian Data Protection Commission (NDPC) regarding inadequate consent procedures for their financial data and excessive data collection, indicating potential violations of the Nigerian Data Protection Act (NDPA). In this scenario, the NDPC plays a central role in addressing these complaints.

Discussion Points:

- What are the initial steps the DPO takes to engage with the NDPC and address the complaints?
- Discuss the DPO's responsibility to evaluate XYZ Bank's compliance with NDPA regulations, specifically regarding consent and data minimization.
- As a DPO, explore the steps you should take if non-compliance is identified. How can the DPO work with the bank's internal teams to rectify the issues and ensure future compliance, while cooperating with the NDPC?

*** A plenary session will be conducted, during which selected participants will have 15 minutes to respond to these questions**



Tips for Trainer

- Clearly outline the learning objectives at the beginning, setting the stage for participants and providing a roadmap for the session.
- Simplify and break down the legal foundations for data processing under the Nigerian Data Protection Act, ensuring participants can grasp the legal framework.
- Provide practical guidance on how to determine which lawful basis to use for specific data processing activities, giving participants actionable insights.
- Highlight the severe consequences of non-compliance with the Nigerian Data Protection Act, creating awareness of legal and reputational risks.
- Equip Data Protection Officers (DPOs) with clear actions to ensure data controllers and processors meet their obligations under the law.
- Provide a step-by-step guide on how to conduct Data Protection Impact Assessments (DPIAs), emphasizing their importance in ensuring compliance.
- Incorporate practical exercises on conducting DPIAs, allowing participants to apply theoretical knowledge in a hands-on manner.
- Clearly state the learning objectives for the section on the role of the Nigerian Data Protection Commission (NDPC), providing clarity on the focus.
- Break down the statutory responsibilities and legal authority of the NDPC, ensuring participants understand the regulatory body's role.
- Examine how the NDPC interprets legal foundations for data processing, offering insights into regulatory perspectives.
- Explore the mechanisms employed by the NDPC to ensure compliance, providing participants with an understanding of regulatory oversight.
- Relate the role of the NDPC to real-world scenarios of data protection compliance, enhancing practical understanding.
- Encourage participants to ask questions and engage in discussions about the NDPC's role, fostering a deeper understanding of regulatory dynamics.
- Emphasize how the NDPC contributes to fostering a culture of compliance, promoting ethical and lawful data processing practices.
- Relate the NDPC's role to broader global trends in data protection, providing a contextual understanding of Nigeria's position in the global landscape.
-

SECTION 6

Technicalities of Data Protection

Topic 1

Privacy Policy, Cookie Policy and Cookie Management

Under this topic, the following key areas shall be discussed:

- Learning Objectives
- Privacy Policy - Significance and Elements
- Creating a Clear and Concise Privacy Policy
- Cookie Policy – Importance and Components
- Understanding Cookie Management

In this training topic, we will discuss the critical aspects of privacy and data management for online platforms. We will explore the significance of Privacy Policies and Cookie Policies, emphasizing the essential elements that must be included to ensure transparency and legal compliance. Participants will gain insights into creating clear and concise Privacy Policies, enhancing user trust. Additionally, we will discuss the importance of Cookie Policies and their components, along with an understanding of effective Cookie Management practices to align with data protection regulations.

Time Allowed: 15 minutes



Privacy Policy, Cookie Policy and Cookie Management

Learning Objectives

Upon completion of Topic 1 “Privacy Policy, Cookie Policy and Cookie Management”, participants shall be equipped with the skills to:



- Create comprehensive and legally compliant Privacy Policies that transparently outline data collection and usage practices.
- Develop Cookie Policies that effectively communicate the purpose and use of cookies, obtaining user consent in accordance with privacy regulations.
- Recognize the significance of Cookie Policies and their essential components, promoting transparency and compliance.
- Understand the principles of Cookie Management, enabling participants to implement effective strategies for cookie consent and user data protection.



Introduction to Privacy & Cookie Policy

In our previous topics, we identified the data principles that identified critical criteria that preserve individuals' privacy and the responsible treatment of their personal information. These principles serve as the foundation for data protection rules, serving as fundamentals for how data is acquired, handled, and safeguarded.

Today, we'll explore how these concepts apply in practice through the lenses of Privacy Policy, Cookie Policy, and Cookie Management.



What is a Privacy Policy?

A Privacy Policy is a critical document that outlines how an organization collects, processes, and safeguards personal data. It is the foundation of transparency and trust with users.

Picture it as a candid conversation between an organization and its users, where the rules of engagement are crystal clear. These policies go the extra mile by emphasizing fairness – they elucidate why data is collected and, importantly, grant you a voice in the matter through consent.

Privacy Policies help organizations to be responsible with data, making sure that they don't collect more than they need. Cookie Management supports this by giving you control over what data is gathered during your online activities.

These policies empower data subjects with the ability to access, amend, or delete their data when necessary, firmly establishing that their data belongs to them.

Key Components of a Privacy Policy

- **Data Collection and Usage Practices:** This is the core of a Privacy Policy. It explains what personal information is collected, how it's collected (through forms, cookies, user interactions), and the specific purposes for which it's used. This component helps individuals understand what they're sharing and why.
- **Consent and User Rights:** Here, the Privacy Policy outlines how user consent is obtained for data processing. It also discusses individuals' rights, such as the right to access their data, correct inaccuracies, request deletion, and object to processing. It's essential to provide a clear process for users to exercise these rights, ensuring they have control over their data.
- **Information Security and Data Retention:** The Privacy Policy addresses the security measures in place to protect personal data. It includes details about data encryption, access controls, and measures to prevent data breaches. Additionally, the policy explains how long data is retained and the criteria used to determine retention periods. It's crucial to show that data is not stored indefinitely and is disposed of when no longer needed.
- **Contact Information:** This component provides individuals with a point of contact for any questions, concerns, or requests related to their personal data. It's important to include a dedicated email address or contact form where users can reach out for privacy-related inquiries. Providing clear and accessible contact information enhances trust and communication.

Sample Privacy Policy

[Your Company Name] ("we," "our," or "us") is committed to protecting your privacy. This Privacy Policy outlines how we collect, use, disclose, and safeguard your personal information. By using our services, you consent to the practices described in this policy.

Information We Collect

We collect information you provide directly, such as your name, email address, and other personal details when you interact with our services.

How We Use Your Information

We use your information to provide, maintain, and improve our services. This includes sending you updates, responding to your inquiries, and personalizing your experience.

Information Sharing

We do not share your personal information with third parties, except as necessary to provide our services or when required by law.

Security

We take security seriously and implement appropriate measures to protect your personal data. We retain your data only as long as necessary for the purposes outlined in this policy.

Your Choices

You can access, correct, or delete your personal information by contacting us. You may also opt out of marketing communications.

Updates to this Policy

We may update this policy periodically. We will notify you of significant changes through our website or email.

Contact Us

For questions or concerns about this policy, please contact us at [Contact Email].



Understanding Cookies and Their Significance in Privacy

Cookies are like digital footprints left behind as you navigate the internet. These small text files, placed on your device by websites you visit, serve various purposes in enhancing your online experience. But, as with any trail of footprints, it's essential to know where they lead and what they reveal.

We will unravel the concept of cookies, exploring their types and purposes, and most importantly, we'll discuss the critical role of Cookie Policies

Cookies

We use cookies and similar technologies to help personalize content, tailor and measure ads, and provide a better experience. By clicking accept, you agree to this, as outlined in our Cookie Policy.

Manage Cookies

Accept All



What is a Cookie Policy?

Cookie Policies are documents or sections of a website's Privacy Policy that inform users about the cookies that are used on a website. They describe the kinds of cookies, their specific functions, and the data they collect. Cookie Policies also tell users how they can manage and change their cookie settings, including giving or withdrawing consent for their use.

In short, Cookie Policies act as a clear communication channel between a website and its users, making sure that individuals know about the cookies in use and their rights regarding data privacy.

Components of a Cookie Policy

- **Types of Cookies:** Cookie Policies inform users about the different kinds of cookies that are used on a website.
- **Purposes of Cookies:** Cookie Policies also describe the specific reasons for using these cookies. They clarify why these small pieces of data are collected. This could vary from improving website functionality, enhancing user experience, and studying user behaviour for website improvement to supporting advertising and marketing activities.
- **Consent Mechanism:** Cookie Policies also tell users how they can give or withdraw their consent for cookie usage. They provide ways for users to manage their cookie settings.

Understanding the Principle of Cookie Management

The principle of Cookie Management refers to the concept of effectively and responsibly managing cookies used on a website or online platform. It involves a variety of practices and guidelines that aim to ensure that cookies are used in a way that follows data protection laws, keeps users informed, and maintains transparency.

- **Consent Management:** A key part of Cookie Management is getting and handling user consent. This means that websites and online platforms must clearly tell users about the kinds of cookies in use, their reasons, and the data they collect. Users should have the option to provide or withdraw their consent for specific cookie categories.
- **Cookie Preferences and Settings:** Cookie Management often involves giving users the option to change their cookie preferences and settings. This lets users pick which types of cookies they are okay with and which they want to block.
- **Transparency and Communication:** A vital principle of Cookie Management is honest communication. Websites should be open and clear about their cookie usage in Cookie Policies. They should provide easy-to-understand explanations about the kinds of cookies, their reasons, and the consequences of user consent or refusal.

Sample Privacy Policy

Here is a sample privacy policy that has some errors and/or omissions. Try to spot them!

Privacy Policy

This privacy policy explains how we collect, use, and protect your personal information when you visit our website or use our services. By using our website or services, you agree to this privacy policy and consent to our data practices.

What information do we collect?

We collect information that you provide to us when you register, purchase, or contact us. This may include your name, email address, phone number, billing address, credit card information, and other details.

We also collect information that is automatically generated when you use our website or services. This may include your IP address, browser type, device type, operating system, pages visited, time spent, and other statistics.

We may also receive information about you from third-party sources, such as social media platforms, advertising networks, analytics providers, and other partners. This may include your demographic information, interests, preferences, and behavior.

How do we use your information?

We use your information for various purposes, such as:

- To provide and improve our website and services
- To process and fulfil your orders and requests
- To communicate with you about our products, offers, and promotions
- To personalize your experience and tailor our content and ads to your interests
- To analyze and measure our performance and effectiveness
- To prevent and detect fraud, abuse, and security issues
- To comply with legal obligations and enforce our terms and conditions

How do we share your information?

We do not sell or rent your personal information to third parties. We may share your information with some of our service providers and contractors.

How do we protect your information?

We have security measures in place to protect your data.

How long your data is retained?

We retain your data for as long as necessary.

What are your choices and rights?

You have some rights to the use of your personal information and we value those rights. To exercise these rights or make enquiries, you can contact us at the email provided below.

You can also manage your cookie preferences and settings through your browser or device. However, some features of our website or services may not function properly without cookies.

Changes to this privacy policy

We may update this privacy policy from time to time to reflect changes in our data practices. We will notify you of any material changes by posting a notice on our website or sending you an email.

Participants are allocated 30 minutes to discuss and analyze the errors in this privacy policy.

Let us Fix it!

▪ **How do we share your information?**

We do not sell or rent your personal information to third parties. We may share your information with some of our service providers and contractors.

The statement "We may share your information with some of our service providers and contractors" in the Privacy Policy is generally vague and lacks necessary detail.

It could be improved in the following ways:

- The Privacy Policy should ideally specify which types of service providers and contractors may have access to the user's information.
- The policy should also clarify why this sharing of information with service providers and contractors is necessary.
- It's important to inform users that the service providers and contractors are also bound by data protection and confidentiality agreements to ensure the security and privacy of the user's information.

▪ **How do we protect your information?**

We have security measures in place to protect your data.

The statement "We have security measures in place to protect your data" in the Privacy Policy is lacking in necessary detail and transparency.

It could be improved in the following ways:

- The Privacy Policy should ideally outline specific security measures and practices in place to protect user data. This may include encryption protocols, access controls, regular security audits, employee training, and any other relevant safeguards.
- The Privacy Policy should indicate whether the organization adheres to recognized data security standards or regulations, such as ISO 27001, to assure users of their commitment to data protection.

- **How long your data is retained?**

We retain your data for as long as necessary.

The statement "We retain your data for as long as necessary" in the Privacy Policy lacks clarity and specificity.

It could be improved in the following ways:

- The Privacy Policy should provide a clear definition of what "necessary" means in the context of data retention. Users should know the criteria or factors that determine the retention period.
- It's important to specify the actual retention periods for different types of data, if applicable. For example, some data may have a shorter retention period than others.






- **What are your choices and rights?**

You have some rights to the use of your personal information and we value those rights. To exercise these rights or make enquiries, you can contact us at the email provided below.

The Privacy Policy should explicitly list the specific rights users have concerning their personal information. Common rights include the right to access, correct, delete, and object to the processing of their data. Each right should be clearly defined.

- The Privacy Policy did not include important contact information, making it difficult for users to communicate directly with the organization. This lack of contact details prevents users from reaching out and asking questions or help about their privacy issues or data handling practices.

Under this topic, the following key areas shall be discussed:

-  **Learning Objectives**
-  **Overview of Third-Party Risks**
-  **Importance of Vendor Due Diligence**
-  **Key Steps in Assessing Third-Party Vendors**
-  **Case Studies and Risk Mitigation**

This training is tailored to provide participants with a comprehensive grasp of third-party risks and equip them with the tools and knowledge needed for effective risk mitigation.

Throughout this training, we will explore the landscape of third-party risks and the critical importance of proactive risk management. We will delve into the significance of vendor due diligence and uncover the practical steps to assess third-party vendors effectively. Real-world case studies will provide insights into actual risks encountered in these partnerships and challenge participants to devise optimal risk mitigation strategies. Our ultimate goal is to empower participants with the expertise to reduce vulnerabilities, bolster data security, and maintain compliance with data protection laws when engaging with third parties.

Time Allowed: 15 minutes



Third-Party Risk Management

Learning Objectives

Upon completion of Topic 2 “Third-Party Risk Management”, participants shall be equipped with the skills to:

- Develop the skills to recognize and categorize risks associated with third-party vendors, partners, and collaborators that have implications for data protection.
- Understand the importance of proactively managing third-party risks to safeguard their organization's data, and ensuring compliance with data protection laws.
- Perform thorough vendor due diligence with a specific emphasis on evaluating a vendor's data protection capabilities, security practices, and adherence to regulatory requirements.





Introduction to Third-Party Risks

In today's business world, it's common for organizations to engage with third-party vendors, partners, and collaborators to meet their business objectives. These partnerships offer numerous advantages, including access to specialized expertise, cost efficiencies, and enhanced capabilities.

Data-related third-party risks are the potential threats that arise when an organization relies on third parties for its operations, products, or services, and these risks extend beyond the organization itself.



Categorizing Data-Related Risks

Data is one of the most valuable and sensitive assets of any organization. However, data can also be exposed to various risks when it is shared, stored, or processed by third parties. These risks can have serious consequences for the organization's reputation, compliance, security, quality, and continuity.

Some examples of common data-related risks that can emerge in third-party relationships are:

- **Data breaches:** The risk of unauthorized or accidental disclosure of the organization's data to external parties due to the lack of adequate security measures or controls by the third party. For example, if a third-party vendor suffers a cyberattack or a human error that exposes the organization's customer data to hackers or competitors, it can result in financial losses, legal liabilities, or customer dissatisfaction.
- **Unauthorized access:** The risk of unauthorized or inappropriate access to the organization's data by the third party or its employees due to the lack of proper access management or policies by the third party. For example, if a third-party partner accesses

the organization's confidential data for its own purposes or shares it with other parties without permission, it can result in a breach of trust, contract, or ethics.

- **Privacy violations:** The risk of violating the privacy rights or expectations of the organization's customers or stakeholders due to the misuse or mishandling of their personal data by the third party.

Depending on the nature and scope of the third-party relationship, different types of data-related risks may apply to different organizations. Therefore, it is important to identify and categorize the specific data-related risks that are relevant to your organization and its objectives.



Risk Assessment Techniques

Once you have identified and categorized the data-related risks that apply to your organization, you need to assess their likelihood and impact. This will help prioritize and manage these risks effectively and efficiently.

Various methods and tools can help you assess these risks. Two common techniques are risk matrices and scenario analysis.

- **Risk matrices:** A risk matrix is a graphical tool that displays the likelihood and impact of different risks on a grid. The likelihood is the probability of a risk occurring, while the impact is the severity of the consequences if it does occur.
- **Scenario analysis:** A scenario analysis is a qualitative tool that explores how different events or situations can affect the organization's data and its objectives. It involves creating plausible scenarios that describe what could happen in the future if certain risks materialize. For example, a scenario analysis could examine how a natural disaster could disrupt the cloud service provider that hosts the organization's e-commerce applications and customer data.



Understanding the Importance of Proactively Managing Third-Party Risks

Proactively managing third-party risks means identifying, assessing, mitigating, and monitoring these risks before they materialize or escalate. It involves establishing a systematic and consistent

process for managing the entire life cycle of the third-party relationship, from selection and contracting to termination and evaluation.

As we have seen, third-party relationships can pose various data-related risks that can affect the organization's reputation, compliance, security, quality, and continuity. Therefore, it is essential to proactively manage these risks to protect the organization's data and ensure compliance with data protection laws.

Some benefits of proactively managing third-party risks are:

- **Enhancing reputation:** By proactively managing third-party risks, the organization can demonstrate its commitment to data protection and ethical practices. This can enhance its reputation and trustworthiness among its customers, stakeholders, regulators, and the public.
- **Ensuring compliance:** By managing third-party risks, the organization can ensure that it complies with applicable data protection laws and regulations in its jurisdiction and in the jurisdictions of its third parties. This can help the organization avoid or reduce legal penalties, fines, or sanctions that may result from non-compliance or violation of data protection laws.
- **Improving security:** The organization can improve its security posture and resilience against data breaches or unauthorized access. This can help the organization protect its confidential and sensitive data from external or internal threats. It can also help the organization reduce the costs and consequences of data breaches or unauthorized access, such as remediation, recovery, notification, compensation, or litigation.
- **Ensuring continuity:** By proactively managing third-party risks, the organization can ensure the continuity and availability of its products or services that rely on or use data from third parties. This can help the organization avoid or mitigate disruption or interruption in its operations, productivity, or revenue due to unforeseen events or circumstances that affect its third parties.



The Role of Vendor Due Diligence in Data Protection

Vendor due diligence is the process of assessing the data protection capabilities and practices of a third-party vendor that provides products or services to an organization or has access to its data.

It is an important step to ensure compliance with data protection laws and regulations, such as the NDPA, and to protect the privacy and security of personal data that is shared with or accessed by the vendor.

The Third-Party Vendor Due Diligence Lifecycle



A step-by-step guide to conducting vendor due diligence in data protection may include the following:

- Identify the vendors that process personal data on behalf of your organization, or that have access to such data. This may include cloud service providers, software as a service (SaaS) provider, payroll Processors, HR services, IT services, etc.

- Conduct a risk assessment to determine the level of due diligence required for each vendor, based on the nature and scope of the data processing activities, the sensitivity of the data involved, and the potential impact of a data breach or violation.
- Perform due diligence on the selected vendors, using various methods such as questionnaires, audits, certifications, references, etc. The due diligence should cover aspects such as:
 - The vendor's data protection policies and procedures
 - The vendor's technical and organizational measures to ensure data security
 - The vendor's compliance with applicable data protection laws and regulations
 - The vendor's sub-contracting and outsourcing practices
 - The vendor's breach notification and incident response protocols
 - The vendor's data retention and deletion policies
- Once the relationship with the vendor is established, ongoing monitoring and auditing are crucial. This involves regular assessments of the vendor's performance, security practices, and compliance with contractual obligations.
- If any risks or issues are identified during the monitoring and auditing phase, the organization works with the vendor to mitigate these risks and ensure compliance with data protection and privacy standards.
- In some cases, the organization may decide to terminate its relationship with a vendor. Having a clear exit strategy is essential to ensure that data and assets are handled appropriately during the termination process.

Interactions and Discussions



The Scenario:

SecureBank, a reputable financial institution, relies on an array of third-party vendors to support its operations. Among these vendors is CyberGuard Solutions, a well-known IT services provider. SecureBank entrusts CyberGuard Solutions with critical IT infrastructure management, network security, and data storage to ensure seamless banking services for its customers.

SecureBank partners with a vendor named CyberGuard Solutions for IT services. A cyberattack occurs, compromising sensitive customer financial data due to vulnerabilities in the vendor's network.

Interactive Discussion Points:

- What data-related risks might SecureBank face in its partnership with CyberGuard Solutions?
- How can the participants identify potential risks associated with financial data and IT services?

Participants will form small groups to brainstorm and present risk mitigation strategies for SecureBank in the event of a data breach. They should focus on immediate actions following a breach. Afterward, they will share their strategies and analyze which ones are the most effective. **(20 minutes)**



Tips for Trainer

- Begin with clearly defined learning objectives, providing participants with a roadmap for understanding privacy policies, cookie policies, and cookie management.
- Emphasize the significance of a privacy policy, detailing its role in establishing transparency and trust with users.
- Break down the essential elements of a privacy policy, guiding participants on how to create a clear and concise document.
- Articulate the importance of a cookie policy and delve into its components, ensuring participants understand the role of cookies in data processing.
- Provide a comprehensive understanding of cookie management, including best practices for users and organizations in handling cookies
- Incorporate interactive elements in the discussion of privacy and cookie policies, such as case studies or examples, to engage participants actively.
- Analyze real-world privacy policies, demonstrating best practices and potential pitfalls to enhance practical knowledge.
- Provide a comprehensive overview of third-party risks, emphasizing the potential impact on data protection and privacy.
- Stress the importance of vendor due diligence in mitigating third-party risks, outlining key considerations in the selection and assessment process.
- Detail key steps and methodologies in assessing third-party vendors, offering practical guidance on risk evaluation.
- Integrate interactive case studies to illustrate real-world scenarios of third-party risks and their mitigation, encouraging participant involvement.
- Discuss effective risk mitigation strategies in the context of case studies, showcasing successful approaches to managing third-party collaborations.
- Provide practical insights into the application of vendor due diligence, linking theoretical knowledge to real-world practices.
- Facilitate discussions on emerging risks related to third-party collaborations, preparing participants for the evolving landscape of data protection.

SECTION 7

Information Security in Data Protection

Topic 1

Data Encryption and Secure Data Handling Techniques

Under this topic, the following key areas shall be discussed:

- Learning Expectations
- Data Encryption and Secure Data Handling
- Advanced Techniques for Secure Data Handling
- Significance of Data Backup And Its Role In Data Security
- Backup Solutions

This training topic will cover the topic of “Data Encryption and Secure Data Handling Techniques.” We will begin with the basics of data encryption and secure data handling, learning the essential principles and methods for protecting sensitive information, as well as advanced techniques that improve data security, such as data masking and anonymization. These advanced techniques are important for maintaining the privacy and integrity of data.

Participants will also learn about the vital role of data backup in data security, ensuring that data is not only secure but also recoverable in case of unexpected events.

To further enhance data security, we will examine secure data transfer methods, such as SSL and VPNs, which protect data as it travels across networks.

Finally, we will stress the importance of data security policies and compliance with data protection laws to ensure that organizations follow the best practices of data security and meet the legal requirements.

By the end of this training, participants will have the knowledge and skills to use data encryption, secure data handling techniques, and comprehensive data security practices.

Time Allowed: 20 minutes



Data Encryption and Secure Data Handling Techniques

Learning Objectives

Upon completion of Topic 1 “Data Encryption and Secure Data Handling Techniques”, participants shall be equipped with the skills to:



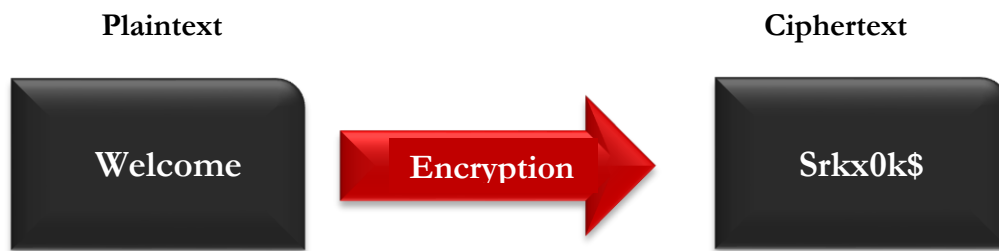
- Understanding of data encryption, including the fundamental principles, methods, and its significance in protecting sensitive information.
- Apply advanced data security techniques such as data masking and anonymization to maintain the privacy and integrity of data in various contexts.
- Recognize the critical importance of data backup in ensuring data security, including strategies for safeguarding data and ensuring its recoverability in unexpected situations.



The Role of Data Encryption in Data Security

Encryption is one of the most effective and widely used methods for data protection. Data Encryption is the process of transforming data (plaintext) into an unreadable form (ciphertext) using a secret key or algorithm. Encryption ensures that only authorized parties can access, use, or modify the data. Encryption also protects the data from accidental loss, corruption, or theft.

HOW ENCRYPTION WORKS



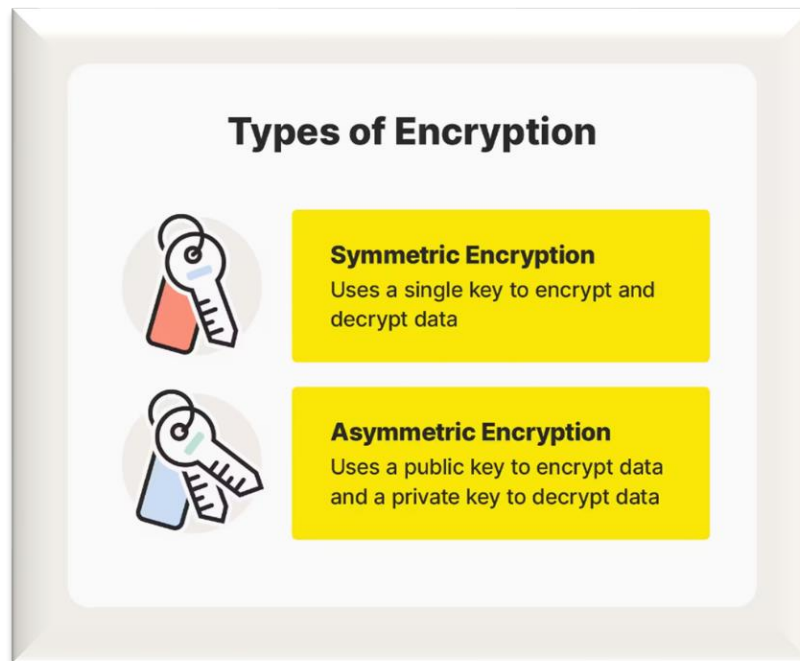
Encryption can be applied to different types of data and at different stages of data processing. For example:

- **Data at Rest:** This refers to data that is stored on a device or a medium, such as a hard drive, a USB stick, or a cloud server. Data at rest can be encrypted using full disk encryption (FDE) or file encryption.
- **Data in Transit:** This refers to data that is moving across a network or a channel, such as the internet, a wireless connection, or an email. Data in transit can be encrypted using secure protocols or standards, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Virtual Private Network (VPN), etc. These protocols encrypt the data before sending it and decrypt it after receiving it.
- **Data in Use:** This refers to data that is being processed or manipulated by an application or a service, such as a database query, a web search, or an online payment. Data in use can be encrypted using homomorphic encryption or secure multi-party computation. Homomorphic encryption allows performing operations on encrypted data without decrypting it. Secure multi-party computation allows performing operations on encrypted data from multiple sources without revealing it.



Types of Encryptions

There are two main types of data encryption: symmetric and asymmetric.



- Symmetric encryption uses the same key for both encryption and decryption. The key must be shared between the sender and the receiver of the encrypted data. Symmetric encryption is fast and efficient but requires secure key distribution and management. Examples of symmetric encryption algorithms are Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (TDES), Twofish, etc.
- Asymmetric encryption uses two different keys for encryption and decryption: a public key and a private key. The public key can be shared with anyone but can only encrypt data. The private key must be kept secret by its owner but can decrypt data encrypted with the corresponding public key. Asymmetric encryption is secure and reliable but slower and more complex than symmetric encryption. Examples of asymmetric encryption algorithms are Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), etc.



Secure Data Handling Techniques

Secure data handling techniques are methods and procedures that help to protect data from unauthorized access, modification, disclosure, or destruction. Secure data handling techniques can be applied to data at rest (stored on devices or servers) and data in transit (transferred over networks or the internet). Some examples of secure data handling techniques are:

- **Data Masking:** is a technique that hides data with altered values. For example, you can replace a value character with a symbol such as “*” or “x”.
- **Data Anonymization:** is a technique that removes all identifiers from a dataset, making it impossible to link the data to an individual. For example, you can remove the house number in an address but keep the road name. Data anonymization preserves statistical accuracy and data integrity but may reduce data utility.
- **Access Control:** This is the process of restricting who can access, modify, or delete data based on their roles, permissions, or credentials. Data access control can be implemented using a system of passwords, biometrics, tokens, or certificates.
- **Data Protection Policies:** These are the rules and guidelines that define how data should be handled, stored, and protected in an organization. Data protection policies can help to establish a common understanding and expectation among employees, customers, and partners about data security.
- **Data Backup:** This is the process of creating and storing copies of data in a separate location or device. Data backup can help to prevent data loss due to accidental deletion, corruption, theft, or natural disasters.



Significance of Data Backup in Data Protection

Data backup is a crucial part of data security. It ensures that any data stored on an organization's system remains safe in the event of data loss or damage, whether caused by hardware failure, software corruption, accidental deletion, or malicious attack.

Nigeria Data Protection Act (NDPA) 2023 requires Data Controllers and Data Processors to implement appropriate technical and organizational measures to ensure the security and confidentiality of personal data.



Data backup can provide several benefits for data protection, such as:

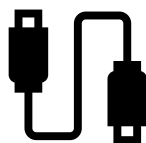
- Preventing data loss in the event your computer or hard drive crashes.
- Protecting data against malware, ransomware, or other cyber threats.
- Helping businesses recover in the event of a successful cyberattack or a natural disaster.
- Acting as a safety net in case you face an unforeseen event that damages or deletes data.
- Helping teams keep operations going without interruption if something happens to your data.

Backup Solutions

Here are some common backup solutions



Cloud Storage



External hard drive



Removable Media



Backup Services

Interactions and Discussions



The Scenario:

You are part of an e-commerce company's security team. Your company handles a large volume of customer data, including personal and financial information. You are tasked with ensuring the secure handling of this data to protect both customers and the organization.

Your e-commerce platform collects customer payment information during the checkout process.

Interactive Discussion points:

- How can you ensure that this sensitive data is securely transmitted from the customer's browser to your servers?
- How do you ensure that only authorized personnel can access customer data while still allowing efficient workflow for different departments?
- How can you provide access to this data without exposing customer details and still maintaining the integrity of the testing process?

*** A plenary session will be conducted, during which selected participants will have 20 minutes to respond to these questions**



Tips for Trainer

- Start with clearly defined learning objectives, outlining what participants will gain from the session on information security in data protection.
- Begin with the fundamentals of data encryption, ensuring participants understand the basics before delving into advanced techniques.
- Provide practical examples and use cases to illustrate how data encryption is applied in real-world scenarios, enhancing practical understanding.
- Delve into advanced techniques for secure data handling, offering insights into cutting-edge practices in data protection.
- Emphasize the critical role of data encryption in overall data security, showcasing its importance in protecting sensitive information.
- Break down various types of encryptions, explaining their strengths, weaknesses, and suitable use cases for each type
- Highlight the significance of data backup in data protection, emphasizing its role in mitigating data loss and ensuring business continuity.
- Discuss different backup solutions available, providing an overview of cloud-based, on-premises, and hybrid options for data backup.
- Incorporate interactive demonstrations of data encryption and secure data handling, allowing participants to witness these processes in action.
- Share case studies illustrating successful implementations of data encryption, offering practical insights into its effectiveness.
- Allocate time for interactive Q&A sessions, allowing participants to seek clarification on complex concepts related to information security.
- Emphasize security best practices in data handling, instilling a culture of responsible and secure data management among participants.
- Address common challenges in implementing data encryption and secure data handling, providing practical solutions for overcoming these hurdles.
- Offer practical tips for effective data backup, covering scheduling, redundancy, and recovery strategies to enhance participants' data protection practices.
- Connect information security practices to regulatory compliance requirements, helping participants understand the legal aspects of secure data handling.

SECTION 8

Cross-Border Data Transfer

Topic 1

Mechanism for Cross-border Data Transfer

Under this topic, the following key areas shall be discussed:

- Learning Objectives
- Concept of Cross-Border Data Transfer
- Impact of the NDPA on Cross-Border Data Transfer
- Safeguarding Data in Cross-Border Data Transfer
- Approaches to Handling Cross-Border Data Transfers

This topic delves into the critical aspect of cross-border data transfer, which involves moving data across national or regional boundaries, whether physically or electronically. It addresses the concept's significance in the global digital economy, the challenges and opportunities it poses for data protection and governance, and ways to safeguard data during these transfers. Additionally, it assesses the pros and cons of various approaches to managing cross-border data flows, highlighting their impact on global data governance harmonization and fragmentation.

Time Allowed: 15 minutes



Mechanism for Cross-border Data Transfer

Learning Objectives

Upon completion of Topic 1 “Mechanism for Cross-border Data Transfer”, participants shall be equipped with the skills to:

- Understand the concept of cross-border data transfer
- Learn how to safeguard data in cross-border data transfer in accordance with the NDPA.
- Compare and contrast the pros and cons of different approaches to handling cross-border data transfers.





The Concept of Cross-Border Data Transfer

Cross-border data transfer is the movement of data across national or regional boundaries, either physically or electronically.

Cross-border data refers to digital information, including personal, business, or other types of data, that is transferred or transmitted across national or regional boundaries. This data transfer can occur through various means, such as the internet, physical storage devices, or other communication methods.



Impact of the NDPA on Cross-Border Data Transfer

The NDPA affects the cross-border transfer of data in several ways. The NDPA aims to protect the rights and interests of data subjects whose data are transferred across borders and to ensure that Data Controllers and Processors comply with the principles and obligations of the NDPA.

Some of the ways that the NDPA affects cross-border transfer of data are:

- The NDPA requires Data Controllers and Processors to obtain the consent of data subjects before transferring their data across borders unless an exception applies. The consent must be specific, informed, and freely given.
- The NDPA also requires Data Controllers and Processors to ensure that the recipient country or organization provides an adequate level of protection for the data, comparable to the standards under the NDPA. The Nigeria Data Protection Commission (NDPC) will publish a list of countries or organizations that are deemed

to provide adequate protection. This list will be available on the official website <https://ndpc.gov.ng/>

- If the recipient country or organization does not provide adequate protection, the NDPA allows Data Controllers and Processors to use other mechanisms to ensure compliance with the NDPA, such as contractual clauses, binding corporate rules, codes of conduct, or certification schemes.
- The NDPA imposes obligations on Data Controllers and Processors to notify the NDPC and the data subjects of any data breach that affects the cross-border transfer of data, and to take appropriate measures to mitigate the risks and consequences of the breach.
- The NDPA grants rights to data subjects to access, rectify, erase, restrict, object, or port their data that are transferred across borders, subject to certain conditions and limitations.
- The NDPA empowers the NDPC to monitor, investigate, and enforce compliance with the NDPA in relation to cross-border transfer of data, and to impose sanctions for violations. The sanctions may include administrative fines, compensation orders, injunctions, revocation of licenses, or criminal prosecution.



Safeguarding Data in Cross-Border Data Transfer

Safeguarding data is the process of ensuring the confidentiality, integrity, and availability of data throughout its lifecycle. Safeguarding data protects it from unauthorized access, use, disclosure, modification, or destruction.

Safeguarding data is especially relevant for cross-border data transfer. However, it also poses challenges to the protection of privacy, security, and sovereignty of data.

Some of the challenges for safeguarding data in cross-border data transfer are:

- Differing or conflicting laws and regulations on data protection among countries or regions
- Lack of transparency or accountability on how data are collected, processed, stored, and shared across borders
- Increased risks of cyberattacks, hacking, theft, or misuse of data by malicious actors or third parties

- Potential violations of human rights or fundamental freedoms of data subjects by foreign governments or entities

Here are some measures that can be taken to safeguard data during such transfers:

- Use strong encryption algorithms to secure data both in transit and at rest.
- Implement Transport Layer Security (TLS) or Secure Sockets Layer (SSL) for secure data transmission over the internet.
- Implement strict access controls and user authentication mechanisms to restrict data access to authorized individuals.
- Deploy DLP solutions to monitor and prevent the unauthorized movement of sensitive data outside the organization.
- Use secure file transfer protocols like SFTP (SSH File Transfer Protocol) or SCP (Secure Copy Protocol) for transferring files securely.
- Implement secure email gateways to protect data shared via email.
- Regularly back up data and implement disaster recovery plans to ensure data availability in case of data loss or system failures during transfer.
- Use cryptographic hashing to ensure that data remains unaltered.
- Only transfer the minimum amount of data necessary for the intended purpose to reduce the risk associated with sensitive information.
- When working with third-party service providers, conduct thorough assessments to ensure they have adequate data protection measures in place.
- Include data protection clauses in service-level agreements (SLAs) with vendors.
- Perform a Data Protection Impact Assessment (DPIA) to evaluate the impact of cross-border data transfer on data subjects' privacy.

Approaches for Cross-Border Data Transfer

There are several approaches to handling cross-border data transfers, each with its advantages and disadvantages. The choice of approach depends on various factors, including the nature of the data, applicable regulations, and business requirements. Here are some of the common approaches:

Binding Corporate Rules (BCRs): BCRs are internal rules or codes of conduct that multinational organizations can implement to govern the cross-border transfer of personal data within their group of companies. BCRs require approval from data protection authorities.

Advantages:

- Provides a unified framework for multinational organizations to transfer data internally.
- Demonstrates a commitment to data protection, which can enhance trust with customers and authorities.

Disadvantages:

- Requires approval from data protection authorities, which can be a lengthy and complex process.
- Limited to data transfers within the organization's group of companies.
- **Consent:** Data subjects can provide explicit consent for their data to be transferred across borders. However, obtaining valid consent can be challenging, and it may not be suitable for all types of data.

Advantages:

- Allows data subjects to have some control over their data.
- Suitable for situations where individuals willingly agree to cross-border data transfers.

Disadvantages:

- Obtaining valid and explicit consent can be challenging and may not be feasible for all data types.
- Relies on the willingness of data subjects, and consent may be withdrawn at any time.

Adequacy Decision: If the Nigeria Data Protection Commission (NDPC) determines that a country or territory provides an adequate level of data protection, data transfers to that destination can proceed without additional safeguards.

Advantages:

- Simplifies cross-border data transfers to countries or territories with approved data protection standards.
- Reduces the need for additional safeguards.

Disadvantages:

- The adequacy determination is subject to change, which can create uncertainty.

- May not cover all data transfer scenarios or destinations.
- **Cross-Border Data Transfer Agreements:** Organizations can negotiate specific data transfer agreements with data recipients in other countries. These agreements outline data protection measures and responsibilities.

Advantages:

- Allows organizations to negotiate specific data protection terms with data recipients.
- Provides flexibility to tailor agreements to meet the needs of the data transfer.

Disadvantages:

- Requires legal and contractual expertise to draft and negotiate such agreements.
- May be time-consuming and costly to establish, especially in complex international settings.

- **Data Localization:** In some cases, businesses choose to store and process data within a specific jurisdiction to comply with local data protection laws. This approach may involve building data centers or using local cloud services.

Advantages:

- Ensures compliance with local data protection laws and regulations.
- Can enhance data security and reduce the risk of data breaches during transfer.

Disadvantages:

- May result in increased operational and infrastructure costs, such as setting up local data centers.
- Limits flexibility in data processing and may hinder cost-efficiency and scalability.

Topic 2

Impact of Data Localization Laws and data protection on global operations

Under this topic, the following key areas shall be discussed:

- Learning Objectives
- Understanding of Data Localization
- Data Localization Laws in Nigeria
- Impact of Data Localization on Global Operations

This topic explores the concept of data localization, with a specific focus on its understanding and application in the context of Nigeria. The detailed exploration of data localization is important because it serves as a specific and in-depth approach to cross-border data transfer, delving into the legal intricacies and implications for global operations, offering valuable insights for businesses navigating the complexities of international data management and compliance. It delves into the intricacies of data localization laws in Nigeria, outlining the legal framework and requirements. Furthermore, the discussion covers the impact of data localization on global operations, highlighting how these regulations can affect organizations conducting business on a global scale. In essence, the topic provides insights into the significance of data localization, its legal aspects in Nigeria, and the broader implications for international business operations.

Time Allowed: 10 minutes



Impact of Data Localization Laws and data protection on global operations

Learning Objectives

Upon completion of Topic 1 “Impact of Data Localization Laws”, participants shall be equipped with the skills to:

- Understand the concept of data localization
- Examine the specific data localization regulations and legal framework in Nigeria
- Assess the implications of data localization on businesses





Data Localization Laws

Data localization, also known as data residency or data sovereignty, refers to the practice of requiring data to be collected, processed, and stored within a specific geographic location or jurisdiction, typically a particular country. In data localization, sensitive or personal data is mandated to remain within the borders of that jurisdiction and cannot be transmitted or stored outside of it without legal or regulatory permission.

DATA LOCALIZATION



Data Localization Laws in Nigeria

Data localization laws in Nigeria are regulations that require data about Nigerian citizens or residents to be collected, processed, and stored within the country, often before being transferred internationally.

The NDPA states that personal data of Nigerian residents shall not be transferred outside Nigeria unless:

- The data subject has given consent to the transfer;
- The transfer is necessary for the performance of a contract between the data subject and the data controller or processor;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller or processor and a third party;
- The transfer is for the benefit of the data subject and it is not practicable to obtain the consent of the data subject, or if obtained, it is likely to be withheld;
- The transfer is made from a register or record that is intended to provide information to the public or is open to consultation by the public;

- The transfer has been authorized by NDPC after ensuring that there are adequate security measures in place in the destination country; or
- The transfer complies with any international treaty or convention ratified by Nigeria.

The NDPA also provides some exceptions for the transfer of personal data to a foreign country, such as:

- When it is required for national security, public order, public health, public morality, or public interest;
- When it is required for historical, statistical, or scientific research purposes and there are adequate safeguards for the rights and freedoms of data subjects;
- When it is required for compliance with any legal obligation or court order; or
- When it is required for the establishment, exercise, or defense of legal claims.



Impact of Data Localization on Global Operations

- **Compliance Burden:** Different countries have varying data localization and data protection requirements. Organizations operating globally must navigate a complex web of regulations and ensure compliance with each country's specific laws. This can result in a significant compliance burden, including the need for legal expertise and ongoing monitoring of changing regulations.
- **Data Security and Privacy:** Data localization laws often require data to be stored and processed within the country's borders. This can impact data security and privacy practices, as organizations may need to establish data centers or infrastructure in each country to meet these requirements. It may also necessitate the implementation of robust data encryption and access controls.
- **Data Transfer Restrictions:** Some countries restrict the cross-border transfer of personal data. This can hinder the flow of data between different locations, impacting global operations and collaborations. To address this, organizations may need to establish data transfer mechanisms such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) to facilitate data transfers legally.

- **Compliance Costs:** Ensuring compliance with data localization and data protection laws can be costly. Organizations may need to invest in technology, legal consultations, and staff training to meet these requirements. Non-compliance can lead to fines and reputational damage, further increasing the cost of doing business.

- **Data Governance and Documentation:** Effective data governance practices and thorough documentation become essential. Organizations must maintain records of data processing activities, consent mechanisms, and compliance measures to demonstrate adherence to data protection laws.

- **Reputational Risk:** Mishandling data localization and data protection can lead to reputational risks. Public perception and consumer trust are crucial for global organizations. Any data breaches or violations of data protection laws can damage a company's reputation.

- **Localization of IT Infrastructure:** To comply with data localization laws, organizations may need to invest in local IT infrastructure, which includes building or leasing data centers, network infrastructure, and hardware. These capital expenditures can affect the cost structure and scalability of global operations.

Interactions and Discussions



The Scenario:

Gen Corporation is a multinational enterprise operating across various countries, including the United States, the European Union (EU), and Asia. The company handles personal data for its customers, employees, and business associates. As part of its worldwide growth, Gen Corporation confronts the task of managing cross-border data transfers while ensuring adherence to diverse data protection regulations.

Gen Corporation must move customer data from its U.S. servers to its EU-based data center to enhance services for EU customers. The EU enforces stringent data protection laws, mandating compliance with GDPR.

The company employs individuals in both the EU and Asia and needs to exchange HR and payroll information between these regions for efficient workforce management.

Interactive Discussion Points:

- What are the merits and demerits of obtaining explicit consent from EU customers for the data transfer?
- Could BCRs be a fitting solution for internal data transfers within the company?

*** A plenary session will be conducted, during which selected participants will have 10 minutes to respond to these questions**

References

List of References

- **The Nigeria Data Protection Act**
https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf
- <https://www.geeksforgeeks.org/what-is-data-encryption/>
- https://www.splunk.com/en_us/blog/learn/data-encryption-methods-types.html
- <https://data36.com/data-anonymization-data-masking/>
- <https://www.ibm.com/topics/encryption>
- <https://www.dot-anonymizer.com/resources/blog-en/data-masking-and-anonymization-understanding-the-different-algorithms/>
- <https://us.norton.com/content/dam/blogs/images/norton/am/types-of-encryption.png>
- https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRO0yNv6Nkxc830b-iK_cgwQg2HknOW-RGw&usqp=CAU
- <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRKMf2dIBz0CpLBYiSLMsoNWROTyVGp0DfVJg&usqp=CAU>
- <https://www.techhiveadvisory.africa/insights/operationalising-the-ndpa-bridging-digital-boundaries-with-cross-border-data-rules>
- <https://aln.africa/insight/cross-border-transfer-of-personal-data/>
- Photo by Ekaterina Bolovtsova on Pexels.co



QUESTION



Tips for Trainer

- Begin with clearly stated learning objectives, providing participants with a roadmap for understanding cross-border data transfer mechanisms.
- Clearly define the concept of cross-border data transfer, ensuring participants understand the intricacies of moving data across international borders.
- Discuss the impact of the Nigerian Data Protection Act (NDPA) on cross-border data transfer, highlighting legal considerations and compliance requirements.
- Emphasize strategies and best practices for safeguarding data during cross-border transfers, addressing security and privacy concerns.
- Foster an interactive discussion on various approaches to handling cross-border data transfers, encouraging participants to share insights and experiences.
- Provide a comprehensive understanding of data localization, explaining the concept and its implications for businesses operating on a global scale.
- Break down the specific data localization laws in Nigeria, ensuring participants are well-versed in the regulatory landscape.
- Facilitate an interactive discussion on the impact of data localization on global operations, encouraging participants to analyze real-world scenarios.
- Discuss challenges related to global compliance with data protection laws, helping participants navigate complexities in different jurisdictions.
- Use case studies or real-world examples to illustrate how data localization laws impact the operations of multinational companies.
- Provide practical strategies for organizations to navigate and comply with data localization laws while maintaining global operations.
- Discuss technologies and tools that can assist organizations in achieving compliance with data localization laws, enhancing practical knowledge.
- Encourage ongoing cross-border compliance training for employees, emphasizing the importance of a well-informed workforce in global operations.
- Relate global operations to broader business strategy, showcasing how effective cross-border data management aligns with organizational goals.

Introduction

The 90 to 365-day plan provides a structured roadmap for organizations to effectively implement data protection controls. This plan outlines a series of steps and actions that can be taken over a period of three months to one year to ensure comprehensive protection of sensitive information within the organization.

During the initial 90 days, the focus is on laying down the foundational elements of data protection. This involves conducting a thorough assessment of the organization's current data protection practices, including an audit of existing data assets, systems, and processes. This assessment helps identify vulnerabilities, compliance gaps, and areas for improvement.

Following the assessment phase, the next step is to develop and implement a tailored data protection strategy. This strategy should encompass policies, procedures, and technical controls aimed at safeguarding data against unauthorized access, disclosure, or misuse.

Key elements of this strategy may include establishing access controls, implementing encryption technologies, and deploying monitoring and detection mechanisms.

Throughout the implementation process, it's crucial to prioritize compliance with relevant data protection regulations, such as NDPA, or industry-specific standards. This involves aligning internal policies and practices with legal requirements, appointing a data protection officer if necessary, and conducting regular compliance audits to ensure ongoing adherence.

Beyond the initial 90 days, the focus shifts to continuous improvement and optimization of data protection measures. This includes ongoing training and awareness programs for employees, regular reviews and updates of data protection policies and procedures, and proactive monitoring of emerging threats and vulnerabilities.

By following this structured 90 to 365-day plan, organizations can systematically strengthen their data protection posture, reduce the risk of data breaches, and enhance trust and confidence among customers, partners, and stakeholders.

What Are My Next Steps Going Forward

1. Assessment of the current state and awareness creation.

Action Plan:

Timelines:

2. Policy Development

Action Plan:

Timelines:

3. Infrastructure and Security

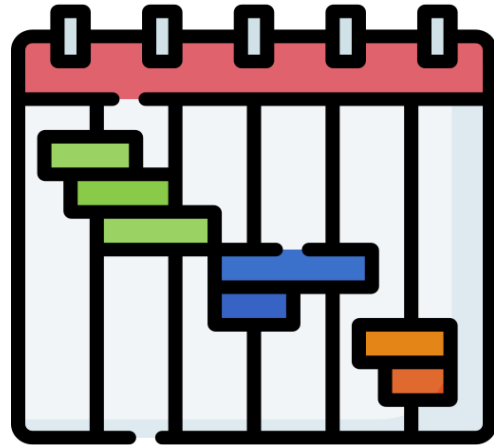
Action Plan

Timelines:

4. Implementation of the Previous Steps

Action Plan

Timelines:



Phase	Objectives	KPIs	Possible timelines
90- days Action Plan			
Assessment and Awareness	Understand the Regulations and Conduct Initial Risk Assessment	Risk Assessment Completion, stakeholder awareness	Weeks 1-2
	Create a Data Inventory	Data Inventory completeness	Weeks 1-2
	Awareness training for Employees	Employee Completion of Training	Weeks 1-2
Policy Development	Develop Data Protection Policy	Policy Completion and Distribution	Week 3-4
	Draft and Update Privacy notices	Notices updated and communicated	Week 3-4
Infrastructure and Security	Implement Basic Security Measures	Security Measure in Place	Week 5-6
	Begin Data Processing Impact Assessment	DPIA initiation and progress	Week 5-6
Implementation	Appoint or Assign Responsibilities to DPO	DPO appointment, roles defined	Week 7-8
	Develop Internal Procedures	Procedures documented and communicated	Week 7-8
	Update Employees contract	Contracts updated with data protection clauses	Week 7-8

180 days Plan				
Process Optimization	Establish process for Handling Data Subjects Rights Requests	Develop a streamlined process for requests	Efficient process for handling request	Months 3-4
	Review and Update Third-Party Agreements	Assess and update agreements with processors	Updated third-party agreements	Months 3-4
Continuous Improvement	Implement Monitoring and review processes	Set up Monitoring processes for compliance	Implemented monitoring processes	Months 5-6
	Develop and Test Incident Response plan	Draft and test an incident Response plan	Tested incident response plan	Months 5-6

365 days Action Plan				
Advanced Security measures	Implement Advanced Security Controls	Enhance security controls based on risks	Implementation of advanced security measures	Months 7-9
	Conduct Regular internal Audits	Perform internal audits to assess compliance	Successful completion of internal audits	Months 7-9
Documentation and Training	Review and Update Documentation, Policies and Procedures	Regularly review and update documentation	Updated documentation and policies	Months 10-12
	Provide advanced training for employees handling sensitive data.	Continuous training for employees	Completion of advanced training sessions	Months 10-12
	Establish processes for timely regulatory reporting	Develop a process for regulatory reporting	Timely regulatory reporting established	Months 10-12
Ongoing				

Continuous Compliance Monitoring	Implement System for Continuous monitoring of Compliance	Set up continuous monitoring mechanism	Ongoing compliance monitoring	Ongoing
	Stay updated on regulatory changes and adjust policies	Regularly monitor and update policies	Timely policy adjustment based on changes	Ongoing
	Conduct periodic reviews	Periodically review and update procedures	Successful completion of periodic reviews	Ongoing
	Consider obtaining external certifications	Explore external certifications for compliance	Attainment of external certifications	Ongoing



End Of Document



NIGERIA DATA PROTECTION ACT



This material was developed under the
AU-EU D4D Hub Project