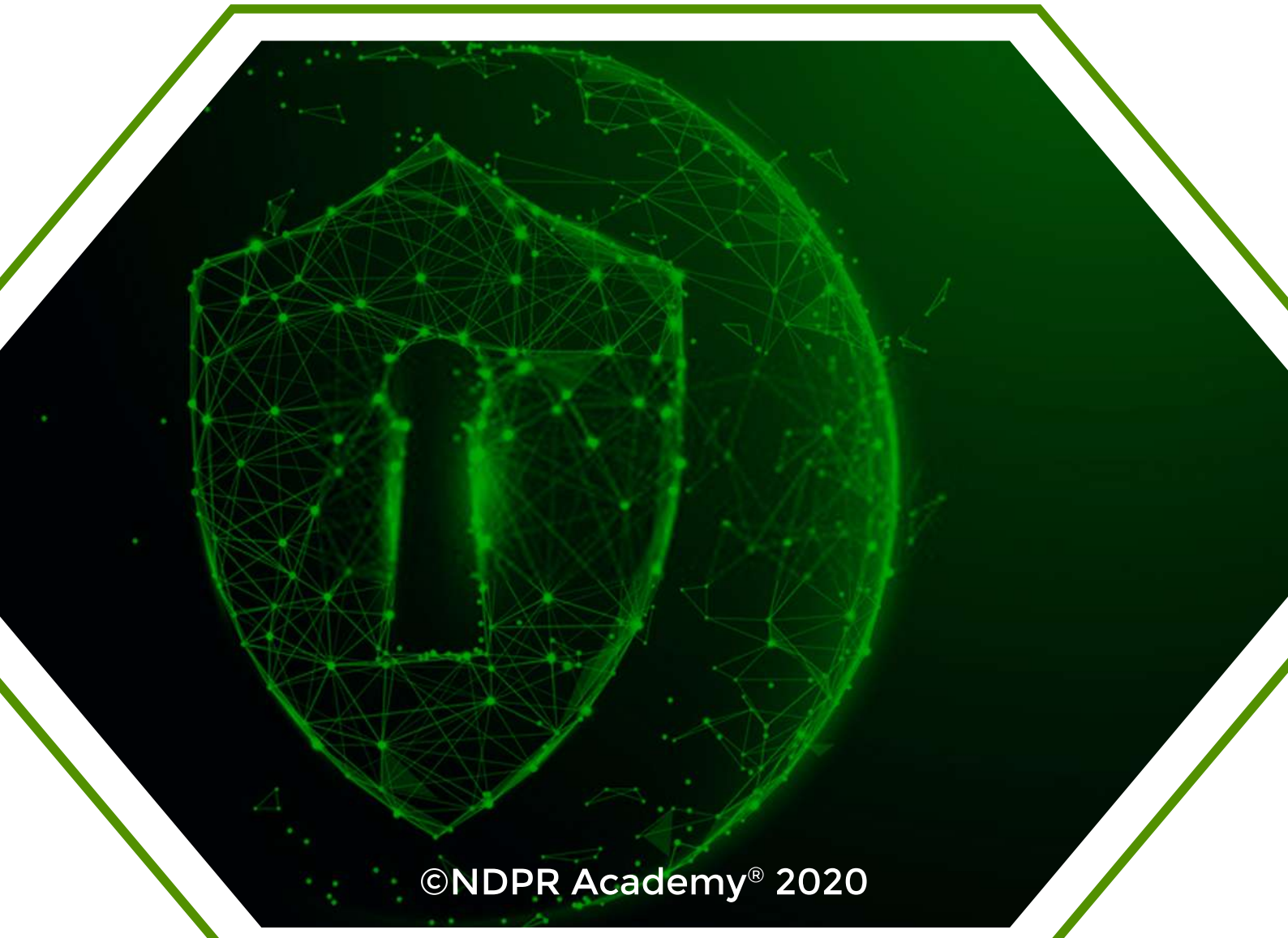
NDPR ACADEMY

NDPR Academy® Practitioner Course

MODULE 3:

PRINCIPLES OF DATA PROCESSING: SECURITY IN FOCUS



Module 3: Overview

In this Module, we will learn about:

- 3.1 Security as a principle of Personal Data processing;
- 3.2 Data Confidentiality, Data Integrity and Data Availability;
- 3.3 Security: Process and System integrity;
- 3.4 the Risk of Personal Data Breaches and Mitigation Strategies; and
- 3.5 some Personal Data Security Concepts.

3.1 Security as a Principle of Personal Data Processing

3.1.1. You may recall from the Foundation Course (Module 2) that the sixth of the 6 principles of Personal Data processing is Security of which we said that Personal Data must be processed in a manner as to guarantee its appropriate security in the context of the confidentiality of, integrity of, and accessibility to the Personal Data. This responsibility includes:

3.1.1.1 protecting Personal Data against unauthorized or unlawful processing; and accidental loss, destruction or damage;

3.1.1.2 using state of the art technical or organizational measures and equipment to protect Personal Data;

3.1.2. NDPR requires that Personal Data must be secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements.[1] A hazard or breach is foreseeable if it is a likely event.

[1]Article 2.1(d) of NDPR

3.1.3. The Data Controller has the unassailable duty to secure all Personal Data within its control. Specifically, NITDA requires Data Controllers and Administrators to develop Personal Data security measures. Such measures must include, but not limited to:

3.1.3.1 protecting systems from hackers;

3.1.3.2 setting up firewalls;

3.1.3.3 secured Personal Data storage with access to specified authorized personnel;

3.1.3.4 employing data encryption technologies;

3.1.3.5 developing organisational policy for handling Personal Data;

3.1.3.6 protection of emailing systems; and

3.1.3.7 continuous capacity building for personnel.[2]

3.1.4 Stricter obligations are placed on Public Institutions who are required to protect Personal Data in any incidence of processing of such data. Specifically, all forms of Personal Data to which Public Institutions have access to are to protected in accordance with the NDPR and any other law or regulation in force in Nigeria.[3]

3.1.5 NITDA will typically need to be comforted by the Data Controller on the controls and processes around access authorisation; the safeguards against corruption and breaches; and the Data Controller or Data Administrator's general approach to security and the implementation of data protection by design. It is accordingly safe to say that NDPR mandates that Data Controllers and Administrators must put in place measures to protect the confidentiality and integrity of Personal Data by setting up a risk management framework.

[2]Article 2.6 of NDPR
[3]Paragraph 2.1 (a) of NPIG

3.1.6 Public Institutions are expressly mandated to to put in place information security structure that ensures the confidentiality, integrity, availability and resilience of Personal Data.[4] Public Institutions that intend to process Personal Data that are in custody of another Data Controller must compulsorily:

3.1.6.1

demonstrate compliance with international information security standards such as ISO 27001:2013 or any similar standard;

3.1.6.2

demonstrate compliance with the provisions of the NDPR;

3.1.6.3

conduct of a DPIA through its DPCO and submit the DPIA Report with NITDA; and

3.1.6.4

retain the services of a DPCO to guide it in its Personal Data processing compliance purposes.[5]

3.1.7 It is important to understand the Personal Data security risks of an organization in order to implement state of the art technical or organizational measures to protect Personal Data. The process of understanding security risks will entail understanding such facts of the Data Controller, as the:

3.1.7.1

nature or value of the Personal Data (Assets) being processed by the Data Controller;

3.1.7.2

size and maturity of the Data Controllers business;

3.1.7.3

vulnerabilities of the Data Controller, its business and the Personal Data it processes;

3.1.7.4

human and natural threats that the Data Controller and Personal Data are exposed on account of vulnerablities; and

3.1.7.5

controls or measures that are required to be put in place on account each and all of the foregoing.

[4]Paragraph 2.6 of NPIG.
[5]Paragraph 2.6 (a) to (d) of NPIG.

3.2 Data Confidentiality, Data Integrity and Data Availability

3.2.1 We earlier established the need for Security of Personal Data in the context of its Confidentiality, Integrity and Availability. These three sub-principles make up the core of the concept of Security according to the NDPR.

3.2.2 **Data Confidentiality:** Confidentiality of data ensures that only authorised personnel have access to the relevant Personal Data. In securing the Personal Data of Data Subjects, access to such data by unauthorised persons could have dire consequences especially in scenarios where such information is intentionally or unintentionally transferred beyond the boundaries it was originally meant to reside. Data Security protocols must ensure that access to the Personal Data of Data Subjects is restricted to only relevant personnel within the Data Controller's space. All Personal Data with the Data Controller must be accorded the status of an organizational asset and must be treated with the utmost care and responsibility. Such data must be protected from any and all conceivable and inconceivable internal, external, deliberate or accidental threats including but not limited to unauthorized access or use, disclosure, theft, loss or destruction.

3.2.3 **Data Integrity:** Integrity of data ensures that the Personal Data is accurate at all times. Personal Data is only as relevant as its accuracy and must be represented as such. Periodic audits must be carried out on all information within the remit of the Data Controller to verify the authencity of the Personal Data of its Data Subjects and relevant updates done. In most cases, relevant periodic conversations must be initiated between the Data Controller and the Data Subjects to verify the accuracy of the Personal Data and must be kept as such at all times. With integrity, we ensure that all Personal Data are accurate and consistent. Data Controllers must validate and ensure the quality of all Personal Data in their possession and such data must be protected from any and all conceivable and inconceivable internal, external, deliberate or accidental threats including but not limited to incorrect changes to information, corruption, hardware error or manipulation.

3.2.4 **Data Availability:** Availability of data ensures that Personal Data is readily accessible by the Data Subject and authorised personnel. Data Availabilty as a subset of Personal Data Security entails that Personal Data be organized in such a way that access to it by authorised personnel and the Data Subject is unhindered and such data is made available upon the adherence to the relevant protocols and policies put in place by the Data Controller. The Data Subjects must at all times have comfort in the fact that their Personal Data is secure and accessible to them at all times. The concept of data availability ensures that all Personal Data is accorded the status of an existential need which must be readily available. Such data must be stored in a manner as to ensure the timeliness and reliability of access and use by authorized persons at all times, including in periods of disaster management or business continuity implementation.

3.3 Security: Process and System Integrity

3.3.1 The risks to the rights and freedoms of Data Subjects on their Personal Data is commonly referred to as privacy risk. Privacy risk management or data protection is recommended to be on a Data Controller's risk management framework as breaches can have financial or reputational impact on the Data Controller. Privacy risks manifest in various forms. We shall however, for the purpose of this module, focus on the risks of: system breaches, collecting excessive Personal Data, disclosing Personal Data without consent, misusing information etc.

3.3.2 The security architecture of the Data Controller or Administrator should be designed with a risk management mind frame. It should be organised in in view of the Personal Data being processed, the likelihood of a security breach and the foreseeable impact of such breach, both to Data Subjects and the organisation.

3.3.3 Organisational roles and responsibilities should clearly be set out in the Data Controller such that information security can easily be demonstrated. There must be appropriate technical and organisational measures or controls in place at each stage of Personal Data processing activities. A RACI matrix is recommended in this regard. It must be clear who, within the organisation, has responsibility for ensuring Personal Data security.

3.3.4 What is an "appropriate technical and organisation measure" is relative to the nature of the Personal Data security risks of the relevant organisation. For example, the Personal Data security risks of a livestock farming business whose database is predominantly filled with with information on its livestock will be different from those of a State tax authority that manages the personal income tax records of the citizens of a State in Nigeria. Accordingly, it is only prudent for an organisation to undertake a Personal Data security assessment to identify its relevant assets, vulnerabilities and threats. While we will deal more on that in the next subsection, suffice to note at this stage that an appropriate technical and organisation measure refers to data breach mitigaton controls that are relative to the organisation. No standard has been set by NDPR as Data Controllers are required to set up and implement the measures or controls that are relative to the risks that they carry.

3.3.5 While documented policies and procedures are important for ensuring the integrity of processes and systems, consistently training personnel on the application of the policies and procedures is a must. Adoption of proven international standards or certifications in process and systems management is recommended. Such certifications include: Cyber Essentials (Plus), the International Standard Organisation's ISO 27001 and the Payment Card Industry Data Security Standard (PCI DSS). Certifications may be used to demonstrate compliance but do not absolve Data Controllers of the responsibility for breaches. A demonstration of compliance may ultimately be factored in the quantification of damages or penalty in the event of breaches.

3.3.6 Save for the relatively few instances where there is a regulatory requirement for an organisation to have a security policy, there is generally no requirement under the NDPR for a Data Controller or Administrator to have a Personal Data security policy. NDPR however mentions that Controllers and Administrators are expected to develop organizational policies for handling Personal Data, that is, the Data Protection Policy;[6] and which in our view should have the Personal Data Security Policy subsumed under it.

Think Time

Coco Plc is about to contract Tide Ltd, a big data analytic company, to help Coco Plc analyse its sales and complaints data of the last 5years with the view of improved service delivery at Coco Plc. Included in the data Coco Plc intends to provide to Tide Ltd are all the Personal Data of customers that came into Coco Plc's possession as a result of its interactions with its customers. The Personal Data included names, addresses, phone numbers, payment card details, dates of purchase and dates of returned products. Coco Plc is rethinking the terms of the proposed contract and contemplating what Personal Data security obligations it should place on Tide Ltd. What do you think Coco Plc should do?

[6]See Article 2.6 of NDPR.

3.4 Risk of Personal Data Breaches + Mitigation Strategies:

3.4.1 Security incidents are events that negatively affect the confidentiality, integrity and availability of Personal Data; essentially, a Personal Data breach. NDPR defines a Personal Data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to processed Personal Data.[7]

3.4.2 Risk management within the context of the NDPR will refer to the process of identifying and managing security incidents (threats) that could severely impact the Personal Data under the control of the Data Controller. ISO explains risks management as involving an analysis of possible occurrences as well as the consequences of such occurrences before deciding on a course of action and the period for which the course of action may be taken in an effort to reduce the risk to a manageable level.

3.4.3 The following concepts are associated with risk management:

3.4.3.1

Asset: This is the object of risk; the object for which we intend to protect against a Threat, given the Vulerabilities of the object. In risk management for Personal Data protection, the Asset is Personal Data. Accordingly, an appropriate risk assessment strategy will begin by identifying the relevant Asset and its Vulnerabilities. A Data Controller that has Sensitive Personal Data in its possession clearly has more to do than one with Personal Data; and the latter has more to do than an organisation without Personal Data (inconceivable right?)..

3.4.3.2

Vulnerability: Vulnerability is the quality or state of an Asset being exposed to the Likelihood of a Threat.

3.4.3.3

Likelihood: This refers to the probability or chances of the occurrence of a Threat, given the Asset and its Vulnerabilities.

3.4.3.4

Threat: A Threat is a negative event that can cause a risk to become a loss. A Threat may be a natural phenomenon such as an earthquake or flood. A Threat may also be man-made such as fire, sabotage, power failure. A Threat is an event that happens to an Asset by exploiting its Vulnerabilities. A Threat may be caused by: gaining unauthorized access to stored information; introduction of false information to mislead users; or denial of service to an authorized user.

[7]See Article 1.3(s) of NDPR.

3.4.3.5

Control: Control are the measures taken to prevent, monitor and mitigate the effect of a security breach incident or its risk. Controls are basically safeguards or countermeasures used to prevent the occurrence of a risk. Control may not always eliminate the risk entirely but may reduce the risk to a manageable level.

3.4.3.6

Impact: Impact is the immediate or eventual effect or consequence of a Threat that has occurred, whether or not a Control was put in place.

3.4.4 An effective and efficient risk management process involves, the:

3.4.4.1 selection of an efficient risk management framework;

3.4.4.2 determination of the level of acceptable risk which involves the identification of threats to assets, identification of vulnerabilities in the organization's system which the threat could expose and exploit, determination of probability of the threat actually exploiting the system's vulnerability and resulting in problems;

3.4.4.3 determination of risk to data subjects by using estimated impact assessment;

3.4.4.4 creation and implementation of a risk treatment plan;

3.4.4.5 maintenance of a Risk Register – a log of events of breaches or attempted breaches detailing the level of such breaches as well as the Data Controller's response to the risk; and

3.4.4.6 review of the risk assessment framework.

3.4.5 Information security threats include but are not limited to: malware, web attacks, ransomware etc. These threats have different targets such as Personal Data, intellectual property, money, commercial information, trade secrets etc. An attack on a system will reveal any vulnerability or flaws in the Data Controller's system. A sound knowledge of the potential threats to Personal Data will involve having people, processes and technologies in place for good risk management.

Think Time

ABC Plc prides itself as Nigeria's foremost software development company. In January 2020 it discovered that the Personal Data of over 100,000 of the employees of some of its Clients have mysteriously wiped off (deleted) from its database. On February 29, 2020, ABC Plc's Head of Compliance told you, as ABC Plc's DPCO, of the incident and asked if everything was fine.

3.4.6 Security breach risks are rife in instances where Personal Data is to be transferred to third parties in order for the third party to perform a defined service. While the third party may have inadequate procedures to secure Personal Data transferred to it, the Data Controller will ultimately bear the liability of any Personal Data breach that occurs thereby. It is accordingly advisable for the Data Controller to mitigate or obviate such risk by undertaking the following:

3.4.6.1 ensure that adequate and updated contractual agreements are in place with the third party;

3.4.6.2 minimise the nature or volume of Personal Data to be provided to the third party;

3.4.6.3 undertake relevant due diligence on the third party and closely monitor their Personal Data processing activities and the contract, in general;

3.4.6.4 subject to the relevant contract, ensure that the third party permanently deletes all Personal Data in its possession as soon as the contract terminates;

3.4.6.5 maintain an up-to-date record of third parties that access, store or process Personal Data available to the Data Controller.

3.4.7 Appropriate measures for mitigating most Personal Data security breaches (whether transferred/transferable to a third party) include:

3.4.7.1 pseudonymising and encrypting Personal Data;

3.4.7.2 ensuring the confidentiality, integrity, availability and resilience of processing systems and services;

3.4.7.3 ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of any physical or technical incident;

3.4.7.4 implementing a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of Personal Data processing.

3.4.8 When eventually they happen, Personal Data breaches must be quickly and effectively investigated and addressed, that is, fixed. Upon detection of a data breach by a Data Administrator, it must immediately notify the Data Controller. Please note that NDPR does not specify a duration. The draft NDPR Implementation Framework however provides that where a Data Controller becomes aware of a Personal Data breach, it should communicate the breach to NITDA and the Data Subject within 72 hours and 7 days respectively.

3.4.9 In reporting a Personal Data breach to NITDA, the Data Controller is required to state the following, the:

3.4.9.1 nature of the breach;

3.4.9.2 categories of Personal Data affected;

3.4.9.3 number of Personal Data and Data Subjects affected;

3.4.9.4 name and contact details of the Data Protection Officer or other contact personnel who can give more information if required;

3.4.9.5 (likely) consequences of the security breach;

3.4.9.6 measures taken or proposed to be taken by the Data Controller to address and mitigate the security breach.

3.4.10 The Data Controller must document Personal Data breaches, effects and remedial actions in a Data Breach Log kept for the purpose.

3.4.11 It is essential to understand the extent of a Personal Data breach incident. Data breach incidents extend to include loss, corruption or unintentional destruction of Personal Data which may be either from natural (such as flash floods, tsunamis, hurricanes etc.) or manmade causes such as technical attacks including viruses or system intrusion, mistakes, accidents, system or process failures.

3.4.12 Processes for data breach incidence response are as important as data breach avoidance itself. The purpose of good data breach incidence management is to appropriately respond to unexpected, disruptive events with the aim of controlling the impact of these events on Personal Data. A Data Controller's ability to detect and respond to data breach incidents in a fast, planned and organized way is important to its longevity and success. There is no total elimination of the probability of a breach, but adequate preparations can be put in place to mitigate the impact of the breach in the event of its occurrence.

3.4.13 A key security risk mitigation strategy is the Data Controller's business continuity plan (BCP). The BCP is a collection of envisioned processes and procedures put in place to rejuvenate services or products back to acceptable delivery forms in a quick and effective manner following the occurrence of a disruptive incident. The disruptive incident may either be natural, for example, destruction by fire, or man-made, for example, a network hack.

3.4.14 The BCP will contain a business continuity and disaster recovery policy or plan. This will detail the steps and processes to protect the business and also systematically recover data in the event of the disruptive incident. In the event of a breach, a good BCP will assure the organization on the sustainability of services and data before, during and after the occurrence of a breach incident. A good BCP will include procedures for preventing data breach incidents. Among these procedures include training sessions and drills wherein the current security measures that are in place are tested against potential breach incidents and vulnerabilities in the system are discovered and fixed.

3.4.15 When a breach of data occurs on an organization's platform, the next steps the organization takes are of crucial importance. Among the essential components of an organization's response to a data breach or attempted data breach is the investigation into the data breach or attempted data breach. Relevant considerations in this regard include such factors as, the:

3.4.15.1 nature or type of breach;
3.4.15.2 nature or type of data that was/is affected;
3.4.15.3 number of data subjects affected;
3.4.15.4 level of risk to rights and freedom of Data Subjects; and
3.4.15.5 remedies to mitigate the effect of the incident.

3.4.16 The process for implementing security investigation involves intrusion management. Below are some related concepts in intrusion management:

3.4.16.1

Avoidance: This involves the use of polices, standards, best practices and tools such as firewalls, access control and encryption to deflect attacks against data. This is a pre-incident measure and involves processes and procedures put into place to avoid incidents of data breach.

3.4.16.1

Assurance: This involves vulnerability testing and systems audit to measure compliance with policies already in place. This concept involves carrying out drills and trainings to detect and address any vulnerability in the system against potential breaches.

3.4.16.3

Detection: This involves steps such as real time logging and interception of breaches or attempted breaches.

3.4.17 The handling of breaches must be methodical, pre-planned and strategic. Experience has shown that good investigation into security breaches should feature thorough reviews of:

3.4.17.1 existing policies, standards and practices;

3.4.17.2 how access controls, incident response rehearsals and drills, vulnerability tests, and real-time intrusion detection and logging have been implemented; and

3.4.17.3 documented past legal issues on the subject of the investigation.

3.4.18 Public Institutions and their Data Administrators have statutorily laid risks mitigation measures that are specific to them. They include the following compliance requirements:

3.4.18.1 all Personal Data databases should, not later than Friday, July 17, 2020, be stored in digital databases with restricted or controlled access;

3.4.18.2 Personal Data are only to be shared with Public Institutions through encrypted formats or other cryptographic methods that protect Personal Data from being easily accessible by unauthorized persons;

3.4.18.3 sharing of Personal Data databases through emails, hard copies and any non-encrypted file formats is prohibited;

3.4.18.4 all Data Controllers with Personal Data of interest to Public Institutions are mandated to create separate encrypted platforms to process such data; they must under no circumstance grant backend access to the databases except where such access is required for conducting criminal investigation by a law enforcement agency or in obedience of a judicial order; and

3.4.18.5 all Personal Data which is to be shared with third parties for processing for purposes of predictive analysis, forecasting, mapping or intelligence gathering must be anonymized or pseudonymized.[8]

3.5 Some Data Security Concepts:

3.5.1 **Information Security Management Systems (ISMS):** These are a set of policies and procedures which are put in place to systematically manage identified data with the Data Controller. ISMS are set to mitigate risks and the impact of security breaches. Among other things, ISMS focus on employee behavior and processes in connection with data and technology and can be configured towards containing Personal Data.

3.5.2 **Risk Register:** A risk register is a tool used to record, assess and monitor risks, particularly risks which had occurred in the past as well as the measures that were used to address such risks. The register must, among other things, contain the date of the occurrence of the breach/risk event, the affected data, the measures taken to mitigate it as well as the result of the application of the implemented measures.

[8]Paragraph 4.0 (a) to (e) of NPIG

3.5.3 **Identity and Access Management:** Identity and access management refers to the process of creating, defining and managing the roles and access privileges individual network users have to access Personal Data. It details the circumstances in which users are granted or denied these access privileges. The users in this regard may be customers (in a customer identity management systems) or employees (in employee identity management systems). The aim of an identity and access management system is the establishment of one digital identity per user on a platform and ultimately security of Personal Data. Identity and access management technologies include but not limited to password management tools, security policy enforcement applications, reporting and monitoring applications and identity repositories.

3.5.4 **Endpoint Security Systems:** Endpoint security systems ensure that devices accessing a Data Controller's network follows a defined level of compliance standards. These standards are as set by the World Wide Web Consortium (W3C). Over the years, endpoint security has evolved from just compliance and has expanded to include antivirus software, threat detection software, investigation and response, device management, data leak protection and other potential security measures.

Endpoint security systems operate on a client-server model. A client-server model is a structure that partitions tasks or workloads between providers of a service – servers and service requesters – and clients. Endpoint security systems operate with a security program controlled by a centrally managed host server with an installed client program which is installed on network drives. Endpoint security systems protects the Data Controller's endpoints from potential threats. It also allows information technology administrators to monitor operation functions and data backup strategies.

3.5.5 **Cloud Security:** Cloud security is the protection of data, applications and software infrastructures involved in cloud computing. Clouds are information technology environments that abstract, collect and share data across a network. Clouds are created to enable cloud computing, which is the process of running workloads within such system. High security concerns such as data leaks and susceptibility to attacks affect traditional information technology systems as well as clouds. Cloud security also involves establishing and maintaining preventive measures to keep data safe as well as tracing and responding to unexpected events.

3.5.6 **Cryptography:** This is the practice and study of techniques for ensuring secure communication. It is focused on the construction and analysis of protocols that prevent third parties or the public from having access to private information or data. It involves many concepts in information security such as data confidentiality, data integrity, authentication and non-repudiation. Cryptography is used in different areas such as electronic commerce, chip-based payment cards, digital currencies, computer passwords and military communications. In cryptography, code is defined as the replacement of a unit of plaintext with a code word. Cryptoanalysis is a term used for the study of methods for obtaining the meaning of encrypted information without access to the key required for unlocking such encryption. It can thus be defined as the study of methods used for cracking encryption algorithms.

3.5.7 We attempt to define below each of the concepts: data authentication and non-repudiation:

3.5.7.1

Data Authentication: Data authentication is the process of confirming the origin and integrity of Personal Data. It is connected to two elements; authentication of the correctness of the entity where information is obtained and validation of the integrity of such information. Any data sent over a properly authenticated and secured channel is considered authenticated. It is good practice to authenticate and ensure data integrity at all times.

3.5.7.2

Non-Repudiation: In data security, non-repudiation may be defined as a service which serves as a means of ascertaining the origin and integrity of data. Non-repudiation refers to a service which provides proof of the origin of data as well as the integrity of data. It makes it difficult to deny the origin of data as well as its authenticity and integrity. Measures such as digital signatures can offer non-repudiation services in online transactions where it is crucial that a party cannot deny the authenticity of their signature on a document or of sending information.

3.5.8 **Encryption:** This is the process of encoding basic text and access to Personal Data which can only be accessed by persons with the decryption key. It is a modern communication system of protecting and limiting access to Personal Data by providing access to a select number of persons. In such a system, there are basically only the sender and the receiver of encrypted

data. The sender sends an encrypted message to the receiver. In order to read the message, the receiver is to have a password or a security key that can be used to decrypt the encrypted messages. Data that has not been encrypted is known as plain text while encrypted data is known as a cipher text. The main purpose of encryption is to protect Personal Data from being accessed by unauthorized persons. It enhances security when Personal Data is being transferred through the internet or any given network. We discuss some of the benefits of encryption below:

3.5.8.1 **Confidentiality**: Encryption enhances confidentiality as the encrypted data cannot be accessed or altered by an unauthorized person.

3.5.8.2 **Accountability Audit:** Encryption makes accountability audit easier. Where Personal Data is leaked, it would be easy to trace the origin of the leak and thus security breaches can efficiently be addressed.

3.5.8.3 **Authentication:** The origin of the encrypted data can be traced and this facilitates authentication on both the source of the data as well as the accuracy of the data.

3.5.9 Encryptions are of three basic types – symmetric, asymmetric and hybrid. Let's summarily explain them below:

3.5.9.1 **Symmetric Encryption:** This is the oldest form of encryption. It involves the sender and receiver of encrypted messages using the same secret key to encrypt and decrypt a message. The key can be a word, a number or a set of random letters.

3.5.9.2 **Asymmetric Encryption:** This type of encryption involves two keys, a public key known publicly and a private key which is known only by the receiver of the encrypted message. The public key is used to encrypt the data while the private key is used by the receiver to decrypt the encrypted data. This type of encryption is slow and usually takes more processing power during encryption.

3.5.9.3 **Hybrid Encryption:** This type of encryption employs both the symmetric and asymmetric types of encryption. It takes advantage of the strength of both encryptions and minimizes weakness.

Think Time

JKL Nigeria Ltd is a Data Controller with over 15million Data Subjects. Emeka Dike was its Head of ICT who was unceremoniously dismissed in December 2019. He did not leave JKL Nigeria Ltd without carting away with the Personal Data of some other employees, including that of the Deputy Managing Director (DMD), who was responsible for his dismissal. Emeka thereafter went to publish the Personal Data of the DMD on social media. The Personal Data in question included private video footages of the DMD obtained from JKL Nigeria's CCTV cameras. The DMD intends to sue JKL Nigeria Ltd. What do you think?

3.5.10 **Hashing:** Hashing is the process of using a mathematical function to convert data into a new data set of fixed values. A hash is a number generated from a set of text and is used to verify that data has not been modified, tampered with or corrupted. No matter how many times a hashing algorithm is executed against data, the hash produced will always be the same if the data is the same. Hashes are created at least twice so they can be compared. Hashing algorithms include but are not limited to the following:

3.5.10.1 Message Digest 5 (MD5)
3.5.10.2 Secure Hash Algorithm (SHA)
3.5.10.3 Hash-based Message Authentication Code (HMAC)
3.5.10.4 RACE Integrity Primitives Evaluation Message Digest (RIPEMD)

3.5.11 Passwords are often stored as hashes. When a new password is created, the system calculates the hash for the password and then stores the hash. Subsequently, when the user authenticates his identity by entering a username and password, the system calculates the hash of the entered password, and then compares it with the stored hash. If the hashes are the same, it indicates that the user entered the correct password which then grants access to the platform. Hashing also provides integrity for messages as it provides assurances to receivers that the messages sent to them were not altered or modified in transit.

3.5.12 **Key Stretching:** Key stretching or key strengthening is a technique used to increase the strength of stored passwords and can protect against attempted breaches and rainbow table attacks. Key stretching techniques add to passwords additional random bits to make them even more complex. 2 common key stretching techniques are summarily explained below:

3.5.12.1
Bcrypt: is based on the blowfish block cipher and is used on many Unix and Linux distributions to protect passwords stored in the shadow password file. Bcrypt secures passwords by adding additional random bits before encrypting the passwords with blowfish. Bcrypt can go through this process multiple times to further protect against attempts to discover the password.

3.5.12.2
Password-Based Key Derivation Function 2 (PBKDF2): uses salts of at least 64 bits and uses a pseudo-random function to protect passwords. Many algorithms such as Wi-Fi Protected Access II (WPA2), Apple's iOS mobile operating system, and Cisco operating systems use PBKDF2 to increase the security of passwords. Some applications send the password through the PBKDF2 process as many as 1,000,000 times to create the hash.

3.5.13 **Zero Trust Model:** This is a security model that establishes and maintains strict access controls by not trusting any user by default. This includes users who are registered and are already inside the network perimeter. It requires strict identity verification or authentication for every person and device trying to gain access to data regardless of whether such person or device is within or outside the perimeters of the network. It ensures that no one is trusted by default as it requires verification from everyone trying to gain access to data on the Data Controller's network. It also gives users only as much access as they would need and as such optimizes each user's exposure to the platform. It exercises strict controls on device access ass it monitors the devices that try to gain access to the Data Controller's network, ensuring that only authorized devices are granted access.

3.5.14 A major characteristic of this security model is its multi-factor authentication (MFA) characteristic. This means that access to data on a platform would require more than one piece of evidence to authenticate the user seeking access and as such, just entering a password would not be enough to gain access to data on the platform with this model. A common example of an MFA is the two-factor authorization used on some social media websites. Typically, users would, in addition to entering a password, also have to enter a code sent to another phone or email, thus providing two pieces of evidence to authenticate their identity.

3.5.15 **ISO 31000 Risk Management Framework:** ISO periodically issues updated standards for risk management. It issued the ISO 31000 in 2018. ISO 31000 is the most commonly used standard for risk management as it provides for principles and guidelines for risk management. The risks management principles covered by the standard include:

- 3.5.15.1 Systematism, structure and timeliness
- 3.5.15.2 Transparency and Inclusivity
- 3.5.15.3 Explicit address of uncertainty
- 3.5.15.4 Dynamism, iteration and response to change
- 3.5.15.5 Facilitation of continuous improvement and enhancement
- 3.5.15.6 Decision making
- 3.5.15.7 Value creation
- 3.5.15.8 Best available information

3.5.16 ISO 31000 is based on 8 management principles which are applicable to different types of organizations. The principles include: Scoping, Risk Assessment, Risk Treatment, Monitoring and Measure, Review, Identification, Analysis and Evaluation.

3.5.17 **Big Data:** These are high-volume, high-velocity or high variety information assets[9] typically used for predictive behavior analytics. To the extent that the relevant data relate to natural persons, big data will have attendant data protection implications, magnified to the size of the Personal Data in question. For example, the process of obtaining consent to process Personal Data contained in a big data pool is conceivably herculean. Another example will be the challenge in keeping the Personal Data in the big data pool accurate.

3.6 Module 3: Summary

3.6.1 Data Controllers and Administrators have the unassailable duty to secure all Personal Data within their control. They should do this by developing Personal Data security measures including a privacy risk management framework which they should implement.

3.6.2 The security architecture of the Data Controller or Administrator should be designed with a risk management mind frame. It should be organised in in view of the Personal Data being processed, the likelihood of a security breach and the foreseeable impact of such breach, both to Data Subjects and the Data Controller or Administrator.

3.6.3 For a Data Controller or Administrator to effectively and efficiently control the risks they are exposed to, there is a need for it to extensively understand the concepts and procedures involved in risk management. Factors such as the proportionality of the risk management framework to a threatened risk, acceptable level of exposure etc., need to be addressed when choosing a risk management framework. When determining the level of risk, it may be exposed to, the Data Controller or Administrator among other things has to set its risk tolerance threshold which will expressly state the level of risk that it can handle.

3.6.4 Relevant Personal Data security concepts include: Information Security Management Systems (ISMS), Risk Register, Identity and Access Management, Endpoint Security Systems, Cloud Security, Cryptography, Encryption, Hashing, Key Stretching, Zero Trust Model, ISO 31000 Risk Management Framework and Big Data.

[9]See: https://www.gartner.com/it-glossary/big-data

Further Reading:

1. 2019 Nigeria Data Protection Regulation[10]
2. National Information Technology Development Act 2007[11]
3. Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020[12]

[10]Available at: http://taxtech.com.ng/download/Nigeria%20Data%20Protection%20Regulation.pdf
[11]Available at: http://taxtech.com.ng/download/NITDA-act-2007.pdf
[12]Available at: https://ndpracademy.ng/resources/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal.pdf

Case Study 1:

Bupa Insurance Services Limited

Bupa Insurance Services Limited manages domestice and global insurance policies. Bupa Global customers can access healthcare services in more than one country, and typically work abroad or travel on a regular basis. Bupa Global's customer relationship management system (SWAN) holds customer records relating to 1.5 million data subjects. SWAN is used to manage claims made by Bupa Global customers under their international health insurance policies.

20 authorised users work in its partnership advisory team (PAT) and 1,351 other users have access to SWAN based on the individual user's business function. However, the 20 PAT members were authorised to make searches, view customer data and run reports from SWAN without restriction. These SWAN reports could then be downloaded and held on shared drives and personal drives in order to respsond to broker enquirires on a "first-time resolution" basis – illustrating the tension between customer satisfaction and information security. At the time, Bupa did not routinely monitor SWAN's activity log and was unaware that the log had a defect that resulted in certain reports not being logged, and other reports being logged inaccurately. This meant that Bupa was unable to detect any unusual activity in SWAN, such as bulk extractions of data.

On 16 June 2017, a staff member in Bupa was informed by an external business partner that personal data of Bupa Global's customers was being offered for sale on the dark web. The advert stated: "Database full of 500,000+ medically insured persons' info from a well-known international blue-chip medical insurance company". A sample of the data was provided to Bupa, which was found to be identical to that held on SWAN.

A PAT member was subsequently discovered to have made unauthorised use of personal data accessed via SWAN to do this. The affected personal data comprised, for each data subject: name, date of birth, nationality, administrative information for the policy and its beneficiaries including membership number, email address, phone and fax number, but no medical information.

Between December 2013 and January 2017, the PAT member also saved three more data sets to their desktop containing information obtained from mandate forms, including payment card details for 15 Data Subjects. On the 18th and 19th of June 2017, Bupa informed the ICO, the Financial Conduct Authority (FCA) and Sussex Police. It also took steps to block the PAT member's log-in details and account, so they could not access Bupa's network and SWAN system. On June 19, the staff member was suspended and on June 20th, Bupa commenced injunction proceedings against him. On June 22nd, the Prudential Regulation Authority (PRA) was informed.

On 10th July 2017, Bupa introduced additional internal security measures and increased its customer identity checks to prevent fraud. On the 12th of July, it begain alerting all its customers to the potential for scam messages and calls. It received 191 complaints from Bupa Global customers about this incident. The ICO also received seven complaints.