Data Protection vis a vis the provisions of the NDPA, whilst drawing comparisons with the GDPR

NBA LAGOS LAW WEEK 2025

NIGERIAN BAR ASSOCIATION
LAGOS BRANCH

ALLNET LAW

GEP LAW
GEORGE ETOMI & PARTNERS


Ito
Onojeghuo
Head of Data Protection
and Consultancy
Hanoba
Etomi
Head of Data Privacy &
Digital Infrastructure

COURSE OUTLINE

- Introduction
- Data Protection Principles
- Lawful Bases for Processing
- Data Subject Rights
- Controllers and Processors

Introduction

Nigeria Data Protection Act (NDPA)

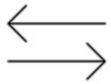
An Act to provide a legal framework for the protection of **personal information**, and establish the Nigerian Data Protection Commission for the regulation of the processing of personal information…

What is Personal Data?

Step 1

Any information...

What qualifies as information?



Step 2

...relating to...

When does information relate to a person?

Step 3

...an identified or identifiable...

What is identity? When is someone identifiable?

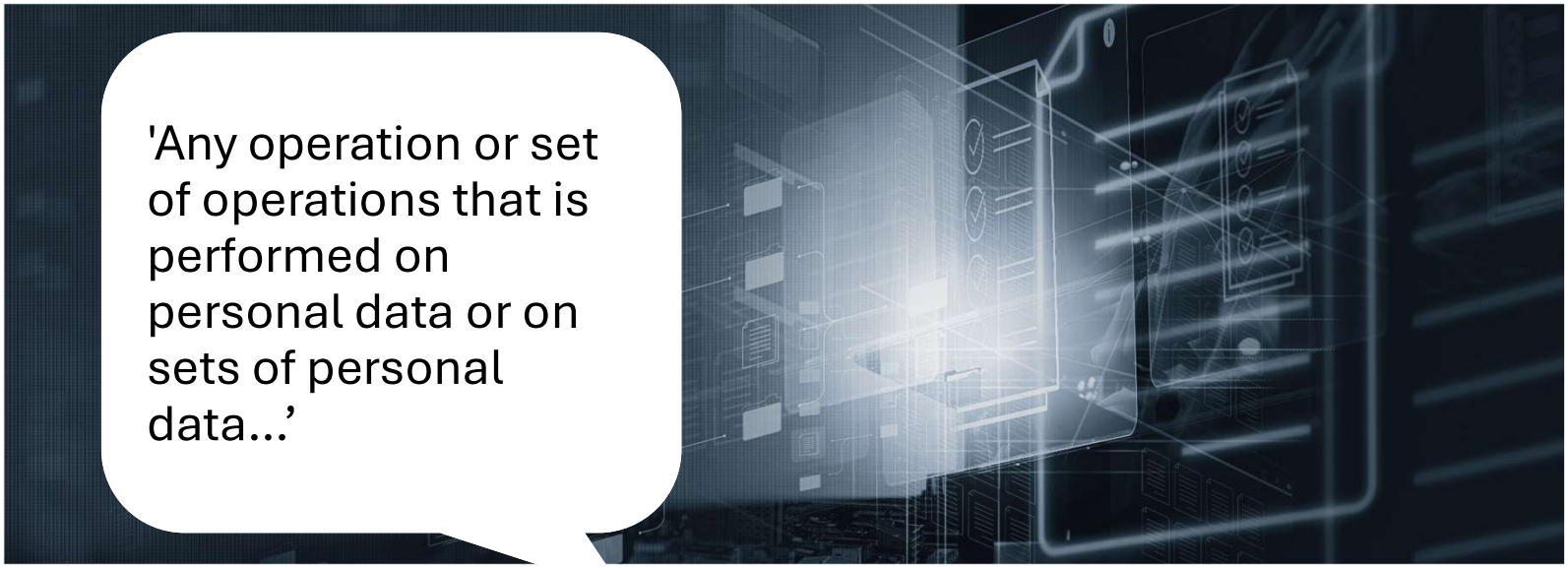
Step 4

natural person.

What is a natural person?

Data Protection Principles

DATA PROCESSING



Article 4(2) of the GDPR

NDPA Principles

NDPA – GAID Art. 15(1)

1. Fairness, Lawfulness & Transparency
2. Purpose Limitation
3. Data Minimisation and Ethics
4. Storage Limitation
5. Data Accuracy
6. Confidentiality, Integrity & Availability
7. Accountability
8. Duty of Care

ENFORCEMENT ACTION

Google hit with £44m **GDPR fine** over ads. **Google** has been **fined** 50 million euros (£44m) by the French data regulator CNIL, for a breach of the **EU's** data protection rules. CNIL said it had levied the record **fine** for "lack of transparency, inadequate information and lack of valid consent regarding ads personalisation". 21 Jan 2019

Google hit with £44m GDPR fine over ads - BBC News

https://www.bbc.co.uk/news/technology-46944696

ENFORCEMENT ACTION

Meta

In July 2024, Nigeria's Federal Competition and Consumer Protection Commission (FCCPC) imposed a $220 million fine on Meta Platforms Inc. for breaching Nigerian data protection and consumer laws which include the principles of fairness, lawfulness and transparency. The investigation, conducted in collaboration with the Nigeria Data Protection Commission (NDPC), revealed multiple violations of the Nigeria Data Protection Regulation (NDPR) and the Federal Competition and Consumer Protection Act (FCCPA).

ENFORCEMENT ACTION / REPRIMAND

Digital Rights Lawyers Initiative

In 2021, the Digital Rights Lawyers Initiative (DRLI) sued the Nigerian government over the collection of Bank Verification Numbers (BVN) for the MSME Survival Fund without a compliant privacy policy. The court found that the government failed to provide necessary information to data subjects, violating NDPR provisions and ordered them to publish a privacy policy and designate a Data Protection Officer.

NDPA Principles

NDPA – GAID Art. 15(1)

1. Fairness, Lawfulness & Transparency
2. Purpose Limitation
3. Data Minimisation and Ethics
4. Storage Limitation
5. Data Accuracy
6. Confidentiality, Integrity & Availability
7. Accountability
8. Duty of Care

Principle: Purpose Limitation - NDPA

GAID Schedule 1(2)

A data controller or data processor shall ensure that personal data is - “collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with this purpose;

Further processing shall not be regarded as compatible if it overrides the rights and interests of a data subject and it has no basis in law or public policy.

Principle: Purpose Limitation - GDPR

GDPR Article 5(1)(2)

Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

However, further processing for:

1. archiving purposes in the public interest,
2. scientific or historical research purposes or
3. statistical purposes

Shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes;

ENFORCEMENT ACTION

In the case of Godfrey Nya Eneye v. MTN Nigeria Communications Ltd, the Nigerian Court of Appeal held that MTN violated the applicant's right to privacy by disclosing his mobile phone number to third parties who sent unsolicited marketing messages.

ENFORCEMENT ACTION

Chukwunweike Araka (the Applicant) was a frequent user of Jumia Food, One such vendor was Eat 'N' Go Ltd. (2nd Respondent), which operates Domino's Pizza. After ordering from the 2nd Respondent via Jumia Food, the Applicant began receiving unsolicited marketing messages from Domino's Pizza. Despite contacting the 1st Respondent to stop the messages and the 1st Respondent relaying this to the 2nd Respondent, the marketing communications persisted.

The Applicant sued both Respondents, alleging a Violation of his right to privacy and a Breach of the data protection principle of purpose limitation.

ENFORCEMENT ACTION

The Court observed that, pursuant to the Nigeria Data Protection Act 2023 (NDPA), the processing of personal data must be restricted to the specific purposes for which consent was obtained. In the instant case, the Applicant had granted consent solely for the processing of his personal data in connection with the fulfilment of his food orders. Consequently, the use of such data for marketing communications constituted a breach of the NDPA.

NDPA Principles

NDPA – GAID Art. 15(1)

1. Fairness, Lawfulness & Transparency
2. Purpose Limitation
3. Data Minimisation and Ethics
4. Storage Limitation
5. Data Accuracy
6. Confidentiality, Integrity & Availability
7. Accountability
8. Duty of Care

NDPA Principles

NDPA – GAID Art. 15(1)

1. Fairness, Lawfulness & Transparency
2. Purpose Limitation
3. Data Minimisation and Ethics
4. Storage Limitation
5. Data Accuracy
6. Confidentiality, Integrity & Availability
7. Accountability
8. Duty of Care

NDPA Principles

NDPA – GAID Art. 15(1)

1. Fairness, Lawfulness & Transparency
2. Purpose Limitation
3. Data Minimisation and Ethics
4. Storage Limitation
5. Data Accuracy
6. Confidentiality, Integrity & Availability
7. Accountability
8. Duty of Care

NDPA Principles

NDPA – GAID Art. 15(1)

1. Fairness, Lawfulness & Transparency
2. Purpose Limitation
3. Data Minimisation and Ethics
4. Storage Limitation
5. Data Accuracy
6. Confidentiality, Integrity & Availability
7. Accountability
8. Duty of Care

ENFORCEMENT ACTION

Plateau State Contributory Health Care Management Agency (**PLASCHEMA**) caused over 45 GB of personal data from 37,000 individuals to be exposed in misconfigured AWS servers. No data protection impact assessment (DPIA) before using cloud infrastructure. No breach response plan; data remained exposed for months. Inability to identify and track responsible parties.

A clear breach of Sections 24 of the NDPA, which mandate organizations to ensure they are not only compliant but can demonstrate compliance at all times.

Car rental manager fined after unlawfully obtaining customer data

Date **16 May 2024**

Type **News**

A former Management Trainee at Enterprise Rent-A-Car UK Limited ("Enterprise Rent-A-Car") has been ordered to pay a fine after admitting he illegally obtained customer data between 18 March 2019 and 1 April 2019.

Initial concerns were raised after Shairaz Saleem, 42, visited his workplace in West Yorkshire outside of his scheduled hours on Sunday 31 March 2019. An internal audit found he'd spent 32 minutes accessing 39 records of customer data in relation to 25 different rental branches.

Following this, Enterprise Rent-A-Car conducted an internal investigation which found Saleem had accessed a number of records containing personal data during the offending period in 2019. He was dismissed for gross misconduct shortly thereafter. The number of records considered to have been unlawfully accessed was at least 213.

Morrisons employee Andrew Skelton jailed over data leak

MORRISONS

A Morrisons employee who posted staff data on the internet as a result of a grudge has been jailed for eight years.

Andrew Skelton, 43, leaked details of nearly 100,000 supermarket staff after he was accused of dealing legal highs at work, prosecutors said.

He then tried to cover his tracks by using a colleague's details to set up a fake email account.

Skelton, of Water Street, Liverpool, denied three charges of fraud but was found guilty at Bradford Crown Court.

The jury heard how he abused his position as a senior internal auditor at the firm's Bradford head office.

He sent information about staff salaries, bank details and National Insurance numbers to several newspapers and posted it on data sharing websites, in a data breach which cost the company more than £2m to rectify.

NDPA Principles

NDPA – GAID Art. 15(1)

1. Fairness, Lawfulness & Transparency
2. Purpose Limitation
3. Data Minimisation and Ethics
4. Storage Limitation
5. Data Accuracy
6. Confidentiality, Integrity & Availability
7. Accountability
8. Duty of Care

NDPA Principles

NDPA – GAID Art. 15(1)

1. Fairness, Lawfulness & Transparency
2. Purpose Limitation
3. Data Minimisation and Ethics
4. Storage Limitation
5. Data Accuracy
6. Confidentiality, Integrity & Availability
7. Accountability
8. Duty of Care

Duty of Care - NDPA

NDPA-GAID Schedule 1(8)

“Duty of care” means the responsibility of a data controller or data processor to carry out data processing professionally and ethically with a view to preventing avoidable harm or injury to the data-subject.

EMPLOYEE PENALTY

Fidelity

In August 2024, the Nigeria Data Protection Commission (NDPC) fined Fidelity Bank ₦555.8 million for processing personal data without informed consent during an incomplete customer account opening process. Fidelity Bank failed to implement adequate safeguards to protect customer data during the account opening process, violating the duty of care principle under the NDPA.

The NDPC imposed a significant fine, emphasizing the importance of data controllers' responsibility to protect personal data.

EMPLOYEE PENALTY

A French court has ordered Ikea to pay a fine of €1m (£860,000; $1.2m) after the Swedish furniture chain was found guilty of spying on staff in France.

Ikea France was accused of using private detectives and police officers to collect staff's private data.

This included illegally accessing their criminal records in order to vet applicants for jobs.

The Ingka group - which owns most of Ikea's stores around the world - has apologised and condemned the practices.

In a statement, reported by Reuters news agency, the company said it had "implemented a major action plan to prevent this from happening again".

NDPA Principles

Article 15(1) of the NDPA-GAID

1. Fairness, Lawfulness & Transparency
2. Purpose Limitation
3. Data Minimisation and Ethics
4. Storage Limitation
5. Data Accuracy
6. Confidentiality, Integrity & Availability
7. Accountability
8. Duty of Care

Duty of Care - NDPA

Knowledge check

An access control system used for building security is later used to pull login data to track employee punctuality. The employees are not informed of this new processing action, and the controller does not keep consistent records of the processing activities.

Which NDPA principles may have been violated?

Lawful Bases for Processing

NDPA-GAID Article 18: When is Consent required?

a) Any direct marketing activity;
b) Processing of sensitive personal data;
c) Further processing that is incompatible with the original purpose
d) For the processing of the personal data of a child
e) Before personal data may be transferred to a country not deemed adequate by the commission
f) Before the data controller makes a decision based solely on automated processing which produces legal effects concerning or significantly affecting the data subject

NDPA: Lawful Bases for Processing Data

NDPA – GAID Art. 16

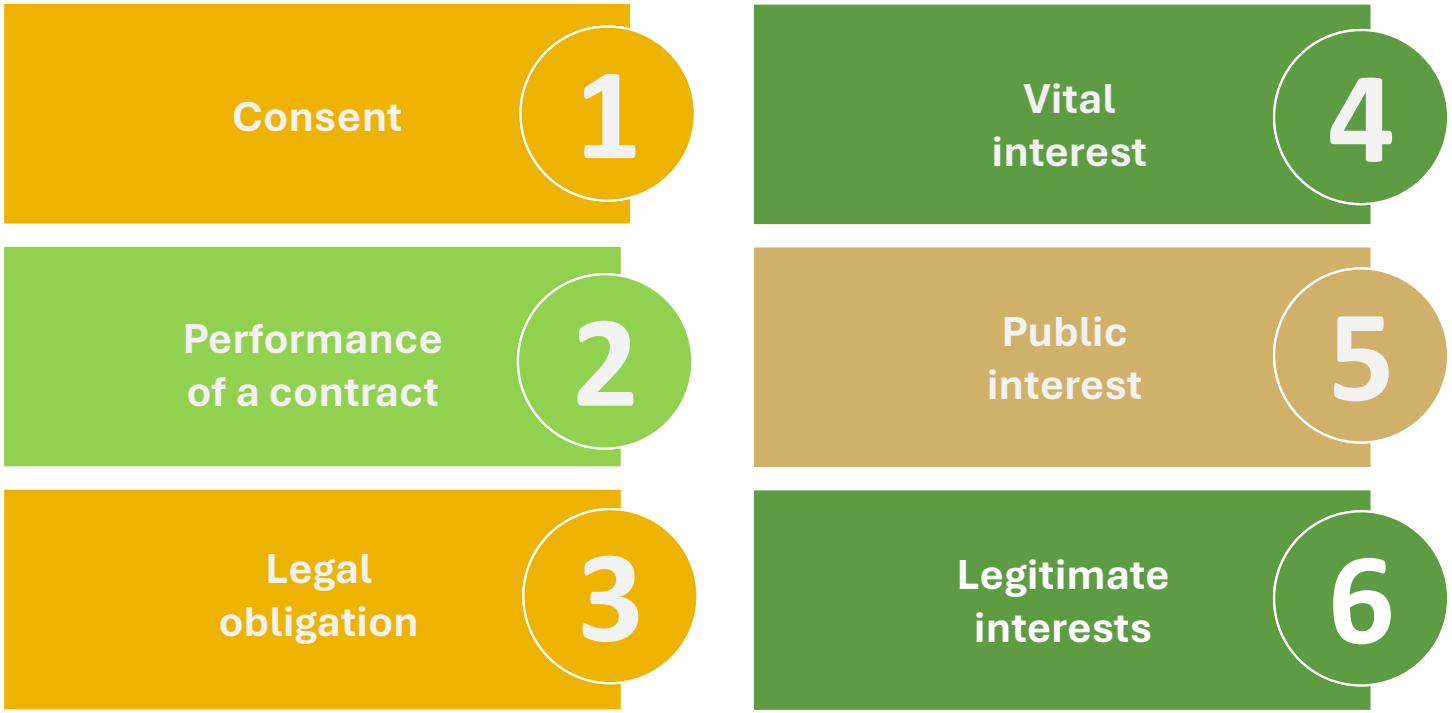
Consent 1

GDPR CONDITIONS FOR CONSENT

- Clear affirmative act
- Freely given
- Specific
- Informed
- Unambiguous indication of wishes
- Demonstrable

NDPA: Lawful Bases for Processing Data

NDPA – GAID Art. 16



NDPA: Lawful Bases for Processing Data

NDPA-GAID Art. 26: Reliance on Legitimate Interest

- A data controller shall cautiously consider reliance on legitimate interest as a lawful basis for data processing and shall be required in a compliance audit to show the basis of its preference.

- Prioritise data ethics and utmost duty of care.

Legitimate Interest Assessment

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn't go ahead with the processing?
- Are you complying with any specific data protection rules that apply to your processing (e.g. profiling requirements)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?
- Will the processing involve the personal data of a child in anyway?
- Do you have an effective means of carrying out age verification?

Legitimate Interest Assessment

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

- Will this processing actually help you achieve your purpose?
- Is the processing proportionate to that purpose?
- Can you achieve the same purpose without the processing?
- Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Legitimate Interest Assessment

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

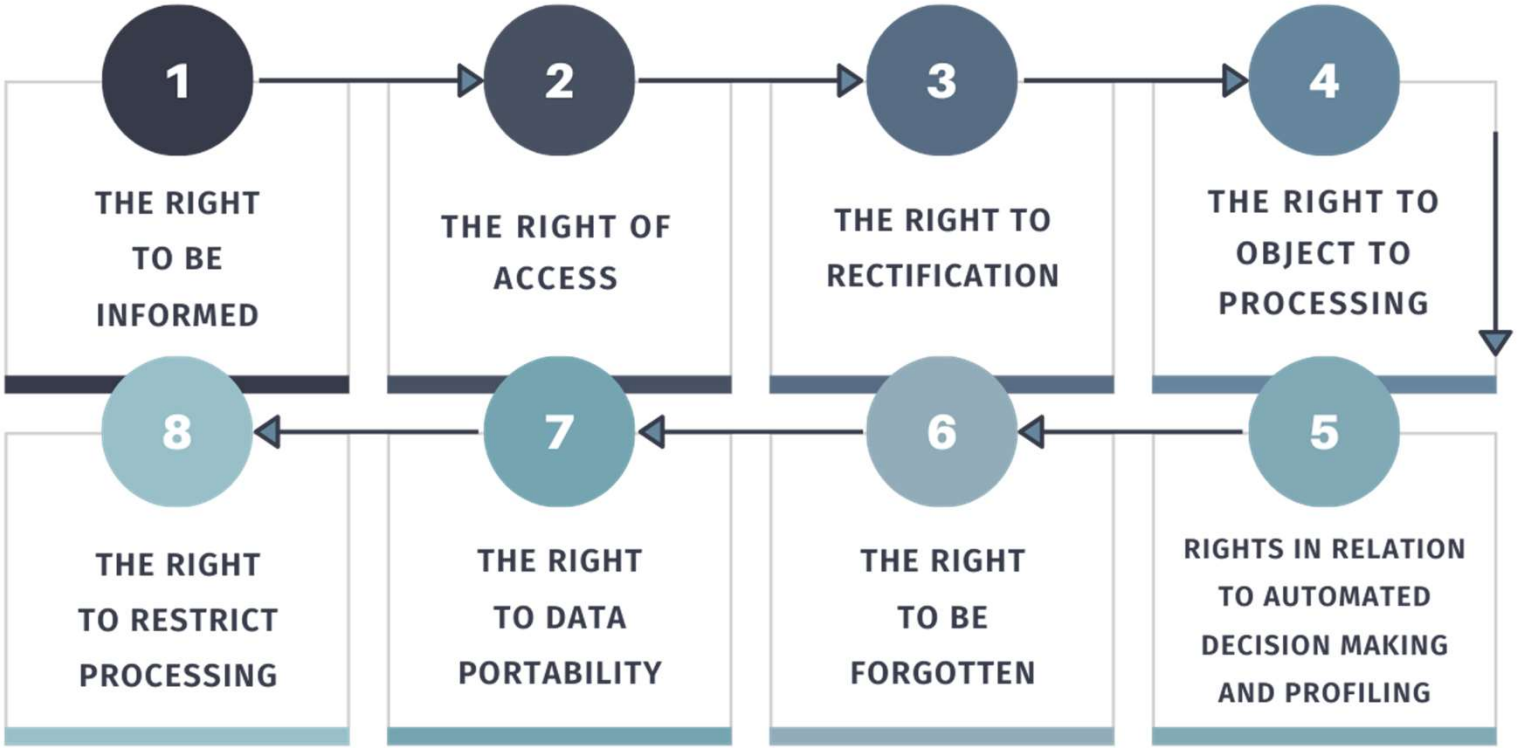
First, use the DPIA **"what to note sections"** in Schedule 4 of the GAID. If you answer yes to any of the questions on what to note, then you need to conduct a DPIA instead to assess risks in more detail.

Nature of the Personal Data

- Is it special category data or criminal offence data?
- Is it data which people are likely to consider particularly 'private'?
- Are you processing children's data or data relating to other vulnerable people?
- Is the data about people in their personal or professional capacity?

Data subject Rights

DATA SUBJECT RIGHTS



www.allnetlaw.co.uk/quiz/master-class

Controllers and Processors

KEY ROLES

CONTROLLER

'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'
GDPR Article 4(7)

PROCESSOR

'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'
GDPR Article 4(8)

VENDOR MANAGEMENT

- Choose reliable processors
- Maintain quality control and compliance throughout the duration of the arrangements
- Frame the relationship in a contract (or other legally binding act)

VENDOR MANAGEMENT

- Controllers must ensure processors implement appropriate technical and organisational measures to secure data
- Security prioritised of controller relationship with potential processor
- Ensure enough controls to protect data shared with processor

DATA PROCESSING AGREEMENT

A data processor is expected to rely on a Data Processing Agreement (DPA) with the data controller in order to carry out data processing on behalf of the data controller.

NDPA - DATA PROCESSING AGREEMENT

A data processor is expected to rely on a Data Processing Agreement (DPA) with the data controller in order to carry out data processing on behalf of the data controller.

Refer to NDPA-GAID Art. 34

GDPR ART 28 - CONTRACTUAL TERMS

- Process on documented instructions only
- Ensure confidentiality
- Comply with International Data Transfer Rules
- Implement appropriate security
- Get controller's consent to engage processors
- Assist with data breach notifications
- Delete or return personal data
- Assist the controller in providing for data subject rights
- Demonstrate GDPR compliance
- Contribute to audits, including inspections

Controller VS Processor

Company X contacts a recruitment company to help advertise for a vacancy on the recruitment company's website.
The recruitment company describes the role and does not disclose the name of Company X on their website.
The recruitment company then shortlists candidates and provides company X with the names and CVs of 3 suitable candidates to be invited for the interview.
--
What is the role of the recruitment company in this scenario?
What is the relationship between both parties and what agreements may be required to fulfil their Data Protection Obligations?

Controller VS Processor

Company X contacts a recruitment company to help select appropriate candidates for a role. As part of the service agreement, the applicants will apply on Company X's website.
Company X shares the details of the applicants with the recruitment company. Then the recruitment company carries out the shortlist and provides Company X with the names and CVs of 3 suitable candidates to be invited for the interview.

What is the role of the recruitment company in this scenario?
What is the relationship between both parties and what agreements may be required to fulfil their Data Protection Obligations?

Thank You