Nigeria - Employment

TABLE OF CONTENTS

June 2020

1. THE LAW

1.1. Key legislation and regulations

- Constitution of the Federal Republic of Nigeria 1999 (as amended) (the 'Constitution'). Section 37 of the Constitution guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. The provisions of Section 37 are very wide, and employers are deemed to be caught by it and are, therefore, required to respect the employee's right to privacy.
- Labour Act, Chapter L1, Laws of the Federation of Nigeria 2004 ('the Labour Act'). The Labour Act prescribes the minimum terms and conditions of employment of workers

(these are employees who generally perform manual labour or clerical work). The terms and conditions of employment of non-workers (employees who perform administrative, executive, technical or professional functions) are primarily subject to the terms of their respective contracts of employment. The Labour Act provides for the maintenance and retention of employment records.

- Nigeria Data Protection Regulation 2019 ('the NDPR'). The NDPR was issued by the National Information Technology Development Agency ('NITDA') and it sets out rules for the collection, processing and transfer of personal data, as well as the rights of data subjects (Nigerian citizens and residents). The NDPR applies to all transactions intended for the processing of personal data and to the actual processing of personal data of data subjects, notwithstanding the means by which the data processing is being conducted or intended to be conducted.
- Cybercrimes (Prohibition, Prevention, etc.) Act 2015 ('the Cybercrimes Act'). This Act ensures the protection of critical national information infrastructure, and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, as well as privacy rights.

Personal data is any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as a MAC address, IP address, International Mobile Equipment Identity number, International Mobile Subscriber Identity number, subscriber identification module, personal identifiable information, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.2. Official guidelines

NITDA has issued the following guidelines:

- Guidelines for Nigerian Content Development in Information and Communications Technology (ICT) 2013 ('the Guidelines').

The purpose of the Guidelines is to provide an enabling environment for local ICT companies, promote the Nigerian ICT industry and provide a framework for the hosting of government data.

1.3. Supervisory authorities

NITDA is the primary agency responsible for data protection in Nigeria.

1.4. Applicable case law

Not applicable.

2. RECRUITMENT AND SELECTION

2.1. General requirements for collection, processing, and disclosure of data

The collection, processing and disclosure of the personal data of prospective employees (who are Nigerian citizens or residents) is governed by the NDPR.

Collection and Processing

The personal data of a prospective employee may only be collected and processed in accordance with a specific, legitimate and lawful purpose consented to by the prospective employee, who must possess the legal capacity to give consent. The processing of personal data is lawful if at least one of the following applies:

- the prospective employee has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the prospective employee is a party, or in order to take steps at the request of the prospective employee prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the organisation is bound;
- processing is necessary in order to protect the vital interests of the prospective employee or of another natural person; and
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official public mandate vested in the controller.

Prior to giving consent, the prospective employee should be informed about the specific purpose of the collection, and of his or her rights under the NDPR (i.e. right to amend inaccurate or incomplete personal data, right to object to or restrict the processing of personal data, right to be forgot-

ten, data portability right, and the right to access and obtain personal data). The request for consent should be presented in an intelligible and easily assessable form using clear and plain language and in a manner that clearly distinguishes it from other matters.

The processing of the prospective employee's personal data must be adequate, accurate and without prejudice to the dignity of the prospective employee, and the employer should ensure that no consent for data collection and processing is sought, given or accepted in any circumstances that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conduct. In addition, the execution or performance of a contract of employment must not be conditional upon the processing of data that is excessive or unnecessary for the performance of that contract.

Where a third party is engaged to process personal data on the employer's behalf, the employer has an obligation to conduct reasonable due diligence on the third party, execute a written contract for the processing with the third party, and ensure that the third party is accountable to the NITDA or a reputable data protection authority offshore.

Further processing of personal data can only be done for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Where the employer intends to further process the personal data for a purpose other than that for which the personal data was collected, the employer shall provide the prospective employee with information on that other purpose and with any relevant further information, prior to that further processing.

Any online medium through which personal data is collected or processed should display a simple and conspicuous privacy policy that the prospective employee can understand. The privacy policy should, among other things, state what constitutes the prospective employee's consent, a description of collectable personal information, the purpose of the collection, the technical methods used to collect and store personal information, access (if any) of third parties to personal data, purpose of the access, available remedies in the event of violation of the privacy policy, the timeframe for the remedy and any limitation of the employer's liability.

An employer is required to develop security measures to protect data. Such measures may include, but are not limited to, protecting systems from hackers, setting up firewalls, storing data securely, access being restricted to specific authorised individuals, employing data encryption technologies, developing organisational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for members of staff on data protection and cybersecurity.

An employer and its third-party data processors owe a duty of care to the prospective employee, and the employer shall be accountable for all acts and omission in respect of data processing.

An employer has a duty to keep personal information in its custody accurate and up to date, and shall, upon request by a prospective employee, delete personal data where one of the following grounds apply:

- the personal data is no longer necessary in relation to the purposes for which it was collected or processed;
- the prospective employee withdraws the consent upon which the processing is based;
- the prospective employee objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data has been unlawfully processed; and
- the personal data has to be erased for compliance with a legal obligation in Nigeria.

Disclosure

Generally, the consent of the prospective employee should be obtained prior to the disclosure of personal data. The consent of the prospective employee is, however, not required where the disclosure is made pursuant to a legal obligation on the employer, or in the interest of defence, public safety, public order, public morality or public health.

2.2. Advertising a position and requirements for data collection regarding CVs, tests, evaluations

An employer is allowed to advertise job vacancies provided the advert does not infringe on any laws or regulations and is not against public morality or public policy.

Please refer to section 2.1. above for data collection regarding CVs, tests and evaluations.

2.3. Requirements and restrictions in relation to background checks

There are no prohibitions against pre-employment checks; however, an employer that intends to carry out such background checks should ensure that it does this:

- in a manner that does not breach the individual's constitutional right to privacy; and

- with the consent of the prospective employee where such check will involve the processing of personal data.

An employer can access a prospective employee's information held by a public institution (i.e. s legislative, executive, judicial, administrative or advisory body of the government) pursuant to the Freedom of Information Act 2011 ('the FOI Act') by submitting an application to that effect. In order to access such information, the employer is not required to demonstrate any specific interest in the information in respect of which the application is made. This right is, however, not absolute, and the public institution may deny access to information where the information contains personal information (defined under the FOI Act as 'any official information held about an identifiable person, but does not include information that bears on the public duties of public employees and officials').

Employers can access publicly available information and obtain the criminal records of the prospective employee from the Nigerian Police Force or the courts, by requesting prospective employees to undergo a police clearance process, or applying to the court for the judgment in respect of a criminal matter. Employers would, however, not be able to access criminal records if such records relate to crimes committed by the prospective employee as a minor (below 18 years).

2.4. Obligations of the employer to protect candidates' right to privacy during interview process

Employers should respect a candidate's constitutional right to privacy and should, therefore, not compel a candidate to divulge personal information or to respond to questions which the candidate considers inappropriate or irrelevant. Sensitive information such as the HIV/AIDS status of a candidate or information which is the subject of a confidentiality agreement, disclosed in the course of an interview should be kept confidential.

2.5. Employer's right to ask questions/request references

An employer has the right to ask questions and request references provided that the questions or requests for references are not discriminatory in nature and do not require the candidate or the referee to divulge confidential or sensitive information as a condition for the recruitment of the candidate. More importantly, the employer must ensure that the questions/requests for reference are relevant for the recruitment process and do not breach the candidate's right to privacy or any applicable law or regulation.

2.6. Candidate's obligation to reveal information

A candidate is under no obligation to reveal personal information.

2.7. Retention of recruitment records

Recruitment records which contain personal data should be stored only for the period within which they are reasonably needed. At the time of collecting the personal data, employers should inform candidates about the period for which their personal data will be stored, or the criteria used to determine the retention period.

2.8. Information to be provided when acting as a referee

A referee can provide information relevant to the request made by the employer, provided the information is not false, discriminatory or libellous and does not breach the referee's legal or contractual obligation.

---

3. EMPLOYMENT RECORDS

3.1. General requirements for collection, processing and disclosure of data

The responses in section 2.1. above apply to the collection, processing and disclosure of the personal data of employees.

3.2. Notification to the employee on collection, processing, access and disclosure

The prior consent of an employee should be sought before collecting, processing, accessing or disclosing his or her personal data. The consent of the employee may be dispensed with where the processing is necessary for:

- the performance of a contract of employment to which the employee is a party, or in order to take steps at the request of the employee to enter into a contract of employment;
- compliance with a legal obligation to which the employer is subject;
- processing is necessary in order to protect the vital interests of the employee or of another natural person; and

- the performance of a task carried out in the public interest or in the exercise of official public mandate vested in the employer.

3.3. Retention of employment records

Employers have an obligation under the NDPR to store personal data only for the period within which it is reasonably needed. At the time of collecting the personal data, employers should inform employees about the period for which their personal data will be stored, or the criteria used to determine the retention period.

With respect to workers, the Labour Act requires employers to retain records for a period of three years post-cessation of the worker's employment.

3.4. Employee rights to information

An employee has the right to access his or her personal data and to obtain information about how the personal data is being processed.

3.5. Disclosure to works councils, state authorities, arbitration courts, etc.

Disclosure of personal data can be made:

- with the consent of the employee;
- pursuant to a legal obligation;
- to protect the vital interest of the employee or another natural person; or
- pursuant to a contractual obligation arising out of the employment documentation with the employee.

4. INFORMATION ABOUT WORKERS' HEALTH

4.1. General rules on processing of workers' health information and exceptions

Employers may, with the consent of an employee, conduct medical tests on such employee. Employers are, however, prohibited from conducting HIV/AIDS tests on an employee, and may only do so if they have obtained the specific prior written consent of the employee to conduct such tests.

Where the employer is in possession of an employee's health information, the information must be held in strict confidence and can only be disclosed with the consent of the employee or in furtherance of a legal obligation or contractual obligation arising out of the employment.

5. EMPLOYEE DATA TRANSFERS

5.1. Legal grounds

Please refer to section 5.2 below.

5.2. Mechanisms for the transfers of data

Transfer within Nigeria

The employer may transfer the personal data of an employee with the consent of the employee. The employer may also transfer the personal data of an employee without the employee's consent, where the transfer is necessary for:

- the performance of a contract to which the employee is party or in order to take steps at the request of the employee prior to entering into a contract;
- compliance with a legal obligation to which the employer is subject;
- the protection of the vital interests of the employee or of another natural person, and
- the performance of a task carried out in the public interest or in exercise of official public mandate vested in the employer.

Transfer outside Nigeria

An employer may transfer the personal data of an employee offshore if:

- it obtains an adequacy decision from the NITDA that the country to which it intends to transfer the data, has adequate data protection safeguards; and the transfer is done subject to the supervision of the Attorney-General of the Federation ('the AGF'). The NITDA has formulated a draft Nigeria Data Protection Regulation 2019: Implementation Framework ('the Framework'), which sets out a list of countries, which in the NITDA's opinion, have adequate data protection safeguards, and to which the personal data can be transferred (the 'White List'). The Framework has not been finalised, and we are aware that the AGF has, as of the date of this article, not approved the White List. The countries that are proposed to be included on the White List are: Angola, Ar-

gentina, Australia, Austria, Belgium, Bulgaria, Brazil, Canada, Cape Verde, China, Croatia, Ghana, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Kenya, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Cyprus, Romania, Serbia, Slovakia, Slovenia, Spain, South Africa, Sweden, Switzerland, United Kingdom, United States of America and Uruguay.

- the employee whose personal data is being transferred has explicitly:
    - been informed of the employer's obligation to transfer the personal data with the AGF's supervision and that such supervision has not been sought;
    - been informed of the possible risks of such transfers; and
    - consented to the transfer; or
- the transfer is necessary for:
    - the performance of a contract between the employer and the employee or the implementation of pre-contractual measures taken at the employee's request;
    - the conclusion or performance of a contract concluded in the interest of the employee between the employer and another natural or legal person;
    - important reasons of public interest;
    - the establishment, exercise or defence of legal claims; or
    - protecting the vital interests of the employee or of other persons, where the data employee is physically or legally incapable of giving consent.

Prior to transferring personal data under paragraphs (b) and (c) above, the employer should ensure that the employee understands through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of the transfer.

Section 14.1 of the Guidelines makes it mandatory for data and information management firms, as well as government ministries, departments and agencies to host government data locally within the country. Data and information management firms are, however, allowed to host government data outside the country with an express approval from the NITDA and the Secretary to the Government of the Federation.

5.3. Sensitive data

Please refer to section 5.2. above.

5.4. Information provision requirements

Please refer to section 5.2. above.

5.5. Notification requirements

Please refer to section 5.2. above.

6. SANCTIONS

6.1. Criminal and civil liabilities

Article 75(4) of the Labour Act provides that any employer who knowingly and with intent to avoid compliance with any provision of this Act, omits to keep any or sufficient record of any particular wages or conditions of employment; or fails to keep a record setting out the particulars of the employee and the date of cessation of employment or a record setting out the particulars of wages and conditions of employment shall be guilty of an offence and on conviction shall be liable to a fine not exceeding NGN 200 (approx. €0.5).

Article 2(10) of the NDPR provides that any person who is found to be in breach of the data privacy rights of any data subject shall in addition to any other criminal liability, be liable to the following:

- in the case of a data controller dealing with more than 10,000 data subjects, payment of the fine of 2% of annual gross revenue of the preceding year or payment of the sum of NGN 10,000,000 (approx. €22,000), whichever is greater; or
- in the case of a data controller dealing with less than 10,000 data subjects, payment of the fine of 1% of the annual gross revenue of the preceding year or payment of the sum of NGN 2,000,000 (approx. €4,500), whichever is greater.

A breach of the NDPR or the Guidelines is construed as a breach of the provisions of the National Information Technology Development Agency Act 2007. A conviction under the NITDA Act for a first offence is punishable with a fine of NGN 200,000 (approx. €450) or imprisonment to a term of one year or to both such fine and imprisonment. A second or subsequent offence is punishable with a fine of NGN 500,000 (approx. €1,100) or to imprisonment for a term of three years or to both such fine and imprisonment.

The Cybercrimes Act provides that notwithstanding any contractual agreement between the employer and the employee, all employees in both the public and private sectors must relinquish or surrender all codes and access rights to their employers immediately upon disengagement from

their employment, and if such code or access right constitutes a threat or risk to the employer, it shall, unless there is any lawful reason to the contrary, be presumed that the refusal to relinquish or surrender such code or access right is intended to be used to hold such employer to ransom. Any employee who without any lawful reason, continues to hold unto the code or access right of his employer after disengagement without any lawful reason shall be guilty of an offence and liable on conviction to 3 years imprisonment or NGN 3,000,000 (approx. €6,723) or both.

Any person that fails to comply with any lawful inquiry or requests made by any law enforcement agency in accordance with the provisions of the Cybercrimes Act commits an offence and shall be liable on conviction to imprisonment for a term of 2 years or to a fine of not more than NGN 500,000 (approx. €1,100) or to both such fine and imprisonment.

ABOUT THE AUTHORS

Jumoke Lambo

Udo Udoma & Belo-Osagie

Jumoke Lambo is a Partner in the firm, and the head of the firm's Data Protection, Telecommunications, Media and Technology teams. She has extensive experience in telecommunications law and general corporate practice with an emphasis on legislative drafting, mergers and acquisitions, foreign investment, corporate restructuring, regulatory compliance and due diligence. Her specialisations include foreign investment, regulatory communications and the capital markets. Jumoke is recognised by the Nigerian edition of Who's Who Legal for her M&A practice. Her work has also been noted in the International Financial Law Review's Expert Guides. She is a fellow of the Centre for International Legal Studies (CILS) and sits on the board of the International LLM Programme of the Suffolk University Law School, Boston, Massachusetts in co-operation with the Eotvos University, Budapest, Hungary and the CILS.

jumoke.lambo@uubo.org

Ozofu 'Latunde Ogiemudia

Udo Udoma & Belo-Osagie

Ozofu 'Latunde Ogiemudia is a Partner in Udo Udoma & Belo-Osagie, where she is part of the firm's Corporate Advisory, Private Equity and Mergers & Acquisitions teams. She is recognised as an extremely resourceful and versatile adviser and has advised on various areas of the law including, corporate and commercial law, private equity, corporate re-structuring and mergers and acquisitions, regulatory compliance, labour and employment, company secretarial practice. Ozofu is a Vice Chairperson of the Nigerian Bar Association-Section on Business Law Committee on Mergers, Acquisitions and Corporate Restructurings, and was also the head of the technical advisory committee that advised the Nigerian Senate on the Company and Allied Matters Act and the Investments and Securities Act.

Ozofu.ogiemudia@uubo.org

Chukwunedum Orabueze

Udo Udoma & Belo-Osagie

Chukwunedum Orabueze is an Associate at Udo Udoma & Belo-Osagie. Chukwunedum is part of the firm's corporate and commercial team, and advises international and local clients on doing business in Nigeria, mergers, acquisitions, foreign investment, government business, employment and regulatory compliance. Some of Chukwunedum's clients include private equity firms and companies in the technology, FMCG, insurance, electric power, banking and finance sectors.

chukwunedum.orabueze@uubo.org

RELATED CONTENT

NEWS POST

Czech Republic: Ministry of Justice presents new whistleblowing act

NEWS POST

Michigan: Microchip Protection Act passes Michigan House

NEWS POST

Australia: ASIC releases whistleblowing guidance

LEGAL RESEARCH

Company auditor obligations under the whistleblower protection provisions (INFO 246) (June 2020)

LEGAL RESEARCH

Company officer obligations under the whistleblower protection provisions (INFO 247) (June 2020)