Data Privacy Protection in Nigeria

By Udo Udoma & Belo-Osagie.

There is presently no specific or comprehensive data privacy or protection law in Nigeria. The only legislation that provides for the protection of the privacy of Nigerian citizens in general terms is the Constitution of the Federal Republic of Nigeria (Promulgation) Act, Chapter C23, Laws of the Federation of Nigeria 2004 (as amended) (the "Constitution"). Section 37 of the Constitution provides that:

"The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected".

Other than this constitutional provision, there is no other law that sets out detailed provisions on the protection of the privacy of individuals in Nigeria. There are however, a few industry-specific and targeted laws and regulations that provide some additional privacy-related protections.

One such industry-specific regulation is the Consumer Code of Practice Regulations 2007 (the "NCC Regulations") issued by the Nigerian Communications Commission ("NCC") - the regulator of the telecommunications industry in Nigeria). The NCC Regulations provide that all licensees must take reasonable steps to protect customer information against ***"improper or accidental disclosure"*** and must ensure that such information is securely stored. It also provides that customer information must ***"not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations".*** Unlike the Constitution, the application of the NCC Regulations is not restricted to Nigerian citizens; they apply to all customer information relating to customers of any nationality that use a licensee's network.

In addition to the NCC Regulations, the National Information Technology Development Agency ("NITDA") which is the national authority that is responsible for planning, developing and promoting the use of information technology in Nigeria, has also issued guidelines on data protection (the "NITDA Guidelines"). The NITDA Guidelines prescribe the minimum data protection requirements for the collection, storage, processing, management, operation, and technical controls for information and is currently the only set of regulations that contains specific and detailed provisions on the protection, storage, transfer or treatment of personal data. The NITDA Guidelines apply to federal, state and local government agencies and institutions as well as private sector organisations that own, use or deploy information systems of the Federal Republic of Nigeria, and also apply to organisations based outside Nigeria if such organisations process personal data of Nigerian residents. The NITDA Guidelines define "personal data" as:

"any information relating to an identified or identifiable natural person (data subject); information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address".

Data controllers (defined as persons which, alone or jointly with others, determine the purposes and means of the processing of personal data) are obliged to prevent any transfer of data to any country that does not ensure an adequate level of protection within the context of the NITDA Guidelines. The NITDA Guidelines also prescribe that in determining the adequacy of the level of protection afforded by another country in relation to the transfer of data, consideration must be given to the nature of the data, the purpose and duration of the proposed processing operation(s), the rules of law, both general and sectorial, in force in the receiving country in question and the professional rules and security measures which are complied with in that country, which should not be lower than the content of the Guidelines. The provisions of the NITDA Guidelines are, however, not mandatory for private companies and only serve as a point of reference for data collectors with respect to the minimum data protection requirements for the collection, storage, processing, management, operation, and technical controls of personal data.

With respect to laws that provide specific data privacy protections, of primary importance is the Child Rights Act No. 26 of 2003 (the "Child Rights Act") which regulates the protection of children i.e. persons under the age of 18 years. The Child Rights Act limits access to information relating to children in certain circumstances. Section 8 of the Child Right Act guarantees every child's entitlement to privacy, family life, home, correspondence, telephone conversation and telegraphic communications, while section 205(2) prohibits the publication of any information that will lead to the identification of a child offender, and requires that the records of child offenders be kept strictly confidential and closed to third parties except in certain limited circumstances.

The provisions of the Freedom of Information Act No. 4 of 2011 (the "FOI Act") also impacts on the protection of the information of individuals in Nigeria. Although the FOI Act was promulgated to, amongst other things, make public records and information more freely available and to provide for public access to public records and information, the FOI Act limits this right of access to information in certain circumstances. Under section 14 of the FOI Act, a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available. Personal information is defined 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". Section 16 of the FOI Act also provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege and journalism confidentiality privilege).

In addition to the foregoing, the Nigerian Courts have also provided some guidance on this matter. In the case of *Habib Nigeria Bank Limited v. Fathudeen Syed M. Koya*[1] which involved an alleged disclosure by a bank of a customer's transactional information, the Court of Appeal held that it is elementary knowledge that the bank owed its customer a duty of care and secrecy. This case indicates that other than the statutory protection afforded to information provided to lawyers, doctors and

[1] [1990 - 1993] 5 NBLR p. 368 at 387

journalists, certain persons (such as banks) owe a duty to maintain confidentiality to their clients - even though such duty is not expressly prescribed by law.
One concern that often arises for employers, in the absence of specific data protection legislation, is in relation to the collection, storage, processing, management and treatment of personal information of employees. This concern, which is common amongst multi-national corporations that usually have a centralised data-base where the employees' personal details are retained, arises from the fact that the language of section 37 of the Constitution is very wide and could be breached in circumstances where it can be established that personal information such as the names, telephone numbers and addresses of employees who are Nigerian nationals have been published or disseminated without the consent of such individuals. In the absence of specific protections under the law, it appears that the only protection available to employers is contractual and as such employers are usually advised to ensure that the terms of each employee's contract of employment (which in Nigeria has been held to include the employees/staff manual) contains a provision pursuant to which an employee consents to the purpose, the treatment and the use by the employer, of any personal information provided by the employee to the employer in the context of the employment relationship.