Key contacts

Cyriacus C. Orlu
Partner,
Dispute Resolution
cyriacus.orlu@templars-law.com

Oghomwen Akpaibor
Managing Counsel,
Corporate & Commercial and METI
oghomwen.akpaibor@templars-law.com

Francis Jarigo
Associate,
Dispute Resolution
francis.jarigo@templars-law.com

TEMPLARS ThoughtLab

Data Retention and Disclosure Conundrum: Negotiating the Complexities of Freedom of Information Act (FoI) Disclosure Requests

Introduction

With the increasing recognition of data protection rights all over the world, the need to regulate data processing and controlling organizations from mismanaging confidential information within their custody has become imminent. To protect personal data, many countries have enacted specific laws and regulations that govern data retention practices. These laws often lay out the types of data that must be retained, the purposes for which it can be used, and the retention periods that must be followed.

In the same vein, as more data privacy laws are enacted, the probability that conflicts could arise on how personal data[1] should be handled or particularly stored, is bound to occur. In Nigeria for instance, the existence of multiple legislations which stipulate various and differing data retention periods, reasonably creates challenges for organizations that are required by law to disclose information (including personal information) in the public's interest. The conflict between the data disclosure laws and the data retention legislations is that the data disclosure laws such as the FoI appear to overlook the minimum retention requirements contained in various data retention legislations for the protection of personal data. Our aim in this article is to provide clarity on this perceived conflict and how organizations can navigate the complexities around retention and disclosure of personal data under Nigerian law.

Data Retention Requirements at a Glance

The Data Protection Act[2] (**DPA**) which is the primary legislation regulating the use of personal data in Nigeria mandates data controllers and processors[3] to ensure that personal data within their custody is retained for not longer than necessary to achieve the lawful bases for which the personal data was collected[4]. Additionally, the DPA places a

[1] Section 1.3 of the Nigeria Data Protection Regulation 2019 ("NDPR") defines personal data as any information relating to an identified or identifiable natural person ('Data Subject'); 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, 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; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.

[2] 2023

[3] Data controller means an individual, Private entity, Public Commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data. Data Processor means an individual, Private entity, public authority or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor.

[4] section 24 (1) (d) of the DPA.

responsibility on data controllers to erase personal data of subjects without undue delay where the personal data is no longer necessary in relation to the purposes for which it was collected or processed, or the data controller has no other lawful basis to retain the personal data.

The Nigeria Data Protection Regulation 2019 ("**NDPR**") Implementation Framework equally provides that in the absence of a retention period, data may be retained for 3 years after the last active use of a digital platform or 6 years after the last transaction in a contractual agreement; or, upon presentation of evidence of death by a deceased's relative or request by the data subject or his/her legal guardian where no statutory provision provides otherwise.[5] In addition to the provisions of the DPA, other specific provisions on data retention in Nigeria are outlined below:

- The Labour Act[6] requires employers to keep records of wages and conditions of employment of their workers, as well as a record showing the name, address of the worker, place of origin, date of birth, next of kin, date and place of engagement, his Nigerian social insurance trust fund number and date of cessation of employment for a period of (3) three years after cessation of employment.
- The Consumer Code of Practice Regulations[7] issued by the Nigeria Communication Commission (NCC) on consumer information[8] requires licensees to retain records of a customer's bill and related charges for a minimum period of twelve (12) months.[9] It also restates the general principles on data protection and privacy contained in the DPA and the NDPR.
- The Guidelines for the provision of Internet service in Nigeria requires Internet Service Providers (ISPs) that supply Internet access services to other ISPs for resale to ensure that their supply agreements include the obligation for the recipient of the services to retain Internet service-related information, including user identification, the content of user messages and traffic or routing data, for a minimum period of twelve (12) months (or such other period as may be directed by the Commission from time to time)[10]. Similarly, licensees of the NCC are required to retain records of consumers bills and related charges for a minimum period of twelve (12) months[11].
- The Credit Information Reporting Act[12], which provides the framework for credit reporting, licensing and regulation of credit bureau, forbids the indiscriminate use of individuals' personal information and further states that the credit bureau shall retain data collected for not less than 6 years from the date it was submitted to it, or provided to the credit user, and then further archive for 10 years before it may be destroyed eventually.[13]
- The Cybercrimes Act requires service providers[14] to keep all traffic data and subscribers' information for a period of two years[15], and
- Under the Companies and Allied Matters Act, 2020 (CAMA), Corporate bodies are generally required to retain records/documents stored in furtherance of the provisions of CAMA for a period of Six (6) years.[16] The records include reports, register of members, shares, minutes, financial statements, balance sheets, resolutions etc.

Disclosure Requirements

Complementary to the data retention provisions discussed earlier, Nigerian law also require organizations to disclose relevant data in their custody when it serves the public interest. In this regard, our focus is specifically on the provisions of the FoI and the Cybercrimes Act because of their non-sector specific application, and the frequency of data disclosure request based on these laws.

The FoI was enacted to give persons, groups and agencies the right to access information in organizations (public and private) that keep information that is of public interest. Although, it mainly applies to public institutions[17], the FoI also applies to private organizations that provide public services, perform public functions or utilize public funds[18]. It not only requires organizations to keep, organize and maintain their records

in a manner that makes them accessible, but it equally mandates organizations to proactively disclose certain categories of information when the interest of the public warrants that they do so. While the FoI attempts to restrict the disclosure of certain classes of information that may qualify as personal data, trade secrets or confidential contractual information, the restriction is not absolute because it is yet subject to any disclosure requests that qualifies as an overriding public interest.

Another legislation that provides for data disclosure is the Cybercrimes Act. The Act provides that every organization shall, when requested by any law enforcement agency, preserve, hold or retain any traffic data, or release any information required to be kept under the Act.[19] Further, the National Identity Management Act which restricts access to the National Identity Database[20] and information therein save where the NIMC's approval is obtained or the data subject consents,[21] states that a data subject's consent may be dispensed with when a request for disclosure of his personal data is necessary in the public's interest, interest of national security, or for the purpose of preventing or detecting crime or for other such purposes regulated by the Commission.[22]

Are organizations legally obligated to disclose information beyond retention limits?

We have often seen cases where officials of various organizations were invited by law enforcement and anti-graft agencies to provide or disclose the personal data of their employees, former employees or contracts which they entered with certain individuals in the past, even at the risk of undermining the privacy rights of the individuals which is almost inviolable under Nigerian law. In the recently decided case of **MTN Nigeria Communication Limited v. Godfrey Eneye**[23], the Nigerian Court of Appeal held that MTN, as a service provider, was in breach of the Respondent's privacy rights when it revealed his registered private MTN GSM mobile phone number to third parties without prior authority or permission from the Respondent.

While it is not unlawful for third parties or law enforcement agencies to request for data disclosure under existing Nigerian laws, a dilemma usually arises where the organizations had already deleted the requested data in compliance with existing data retention legislations and as such, no longer has custody or control over the requested data. As a matter of fact, in addition to bearing liability for unauthorized disclosure of personal data to third parties, many organizations have been made to

[5] Article 9 of the NDPR 2019 Implementation Framework.
[6] Section 75 of the Labour Act, 1971
[7] 2007
[8] Section 48.
[9] Section 23.
[10] Paragraph 16 of the Guideline for Provision of internet service in Nigeria
[11] Section 21 (e) of this Regulation
[12] Credit Information Reporting Act, 2017
[13] Section 5
[14] Section 58 of the Cybercrimes Act 2015 defines service providers as: (i) any public or private entity that provides to users of its services the ability to communicate by means of a computer system, electronic communication devices, mobile networks; and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.
[15] Section 38 (1) of the Cybercrimes Act 2015.
[16] Section 864 of CAMA.
[17] (Sections 2(7), 29(9) and 31 of the FOI define "public institutions" to include legislative, executive, judicial, administrative or advisory body of the government, including boards, committees or commissions of the state; any subsidiary bodies of the above, including but not limited to committees and sub-committees which are supported in whole or in part by public fund or which expends public funds; all companies in which the government has controlling interest)
[18] See Sections 2(7), 29(9) and 31 of the Freedom of Information Act, 2011.
[19] Section 38 (2) and (3)
[20] Established pursuant to Section 14, NIMC Act, 2007. Schedule 2 of the Act lists the contents of database that the Commission keeps.
[21] Section 26 (1), NIMC Act, 2007
[22] Section 26 (2) and (3), NIMC Act, 2007
[23] Court of Appeal, Abuja Division, Appeal no. CA/A/689/2013 – Judgement delivered on 12 May 2017.

suffer undue pressure and intimidation to disclose personal data of their personnel beyond the permitted retention limit.

The position of Nigerian law as contained in the NDPR is that where an organization destroys data that is no longer in use or necessary, it will not be considered to have breached the privacy rights of a data subject. In other words, an organization can destroy data that is no longer in use. The NDPR, which is a subsidiary legislation to the DPA, provides that "*Personal Data that is no longer in use or which has been retained beyond the requisite statutorily required storage period, shall be destroyed in line with global best practices for such operations. Evidence of destruction of data shall be a valid defence against future allegation of breach by a Data Subject*"[24] The implication of this provision of the NDPR is that, where there is evidence of destruction of data that an organization previously had, the organization should be exonerated from liability if a claim is brought for privacy breach by a data subject or if it is unable to comply with a subsequent request for data disclosure. It would be also impracticable to compel an organization to provide data/information that it no longer has in its custody.

In other jurisdictions where common law applies, such as Australia, inoperability of data is considered a barrier to data disclosure. Inoperability and compatibility issues due to an organization's outdated information technology systems and software is a barrier to information sharing[25]. Likewise, in the United Kingdom where many organizations regularly receive requests[26] from the Police to share personal data held about their employees, clients or visitors for purposes of investigations, organizations are advised to be wary of sharing personal data of their subjects, even if the requestor is the Police[27] because of the potential risks associated with non-compliance with the General Data Protection Regulation (GDPR) or Data Protection Act, 2018. In fact, except in cases where the request is in the form of a warrant, Police request for data disclosure is not a mandatory demand for information in the United Kingdom.[28]

Seeing that there is a dearth of judicial pronouncement on the issue of disclosure of personal data beyond retention limits under Nigerian law, the view of the writers is that when Nigerian Courts are presented with an opportunity of resolving this perceived conflict between an organization's duty of erasing data in compliance with the data retention laws and keeping such data beyond the permitted period in order to be able to comply with the data disclosure laws, the Courts will adopt the rule of interpretation that requires general statutes to yield to special ones and will absolve organizations that erase such data in compliance with the data retention laws from liability. In other words, the Courts are more likely to follow the specific provisions of the data retention legislations as against the umbrella disclosure requirements in the FoI and kindred statutes. Organizations cannot be compelled to and will not be liable if they are unable to provide or disclose data/information that they do not have in their custody.

[24] Paragraph 8:3
[25] https://ovic.vic.gov.au/privacy/resources-for-organisations/information-sharing-and-privacy/
[26] This could be a request for information about employees, customers or a copy of CCTV recording.
[27] Handling Requests for Information from the Police | Thorntons Solicitors (thorntons-law.co.uk)
[28] ibid

Conclusion

In the final analysis, our view is that organizations should retain data of subjects only for the period that it is necessary in relation to the purposes for which the data was collected or where it has no other lawful basis to retain such data, like in furtherance of Court orders or for purposes of investigation by law enforcement agencies. As for organizations that erase data of their subjects in compliance the data retention legislations and can provide evidence of erasure/destruction of such data, they can strongly argue that they are exempted from liability where they are unable to comply with data disclosure requests, as it is within their rights to do so.