ÆLEX

ARTICLE SERIES

THE RIGHT TO BE LEFT ALONE – EXAMINING THE IMPACT OF THE NIGERIA DATA PROTECTION REGULATION ON COLD MARKETING

JANUARY 2021

www.aelex.com

INTRODUCTION

The majority of people with a mobile phone or access to the internet have received unsolicited emails or calls at some point in time from telemarketers.

Generally known as cold marketing, it is the practice whereby a sales-person emails or calls a prospect they have never met and explores whether there is a need for their product or service.

While cold marketing has been a tool used by marketers for decades, the recent awareness in data protection and privacy, heightened by the issuance of the General Data Protection Regulation ("GDPR") by the European Union (EU) in 2018 may have affected this concept in recent times, particularly in relation to access to the data of consumers.

Indeed, the GDPR introduced sweeping changes in the data protection and privacy laws in the EU and also, impacted how other nations and businesses interact and do business with entities in the EU.

In addition, Nigeria, amongst other countries, took a cue from the GDPR and issued a similar regulation called the Nigeria Data Protection Regulation ("NDPR") which introduced changes to its laws to meet the realities of the impact that the GDPR could bring. The Nigeria Data Protection Regulation ("NDPR") was issued in January 2019 in tandem with international best practices on data protection and privacy.

In this article, we examine the NDPR and its impact on cold marketing, using cold emailing as a case study in Nigeria.

COLD EMAILING.

A cold email is an unsolicited email sent to a stranger to gain a benefit in terms of favour, sales, opportunity or for any other reason. Cold emailing is a widespread practice, ranging from students sending emails to HR professionals for internships, professionals sharing their resumes to prospect employers to marketers sending emails to gain publicity and traction for their new products.

Cold emailing is a common advertising tactic that was easy to implement in the past. This was because individuals or organisations who sent cold emails relied on the personal data of the consumer market for a wide range of activities. The rise in the use of technology has particularly made personal data easily accessible. However, with the NDPR, more organisations must now be data protection compliant. This limits the rampant cold emailing practice, despite the easy access of personal data.

The introduction of the NDPR

In Nigeria, the right to privacy, (sometimes referred to as the right 'to be left alone') is entrenched in **Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended)**, which provides that *the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communication is hereby guaranteed and protected.*

It is important to note at this juncture that other than the Constitution, the most relevant legislative instrument on data protection is the Nigeria Data Protection Regulation ("NDPR") issued by the National Information Technology Development Agency ("NITDA"). NITDA also issued the Data Protection Implementation Framework (DPIF)[1] which serves as a guide to data protection implementation in Nigeria.

Personal data under the NDPR

The NDPR defines personal data to mean: *"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 and others[2]".*

[1] Article 9 of the Data Protection Implementation Framework
[2] Section 1.3 of the NDPR.

The inference drawn from this is that information such as a person's name, email address, phone number, etc constitutes personal data. While certain persons, designated as data controllers by the NDPR, may obtain such information with the consent of the data subject (the person whose data is being processed) and for a purpose, the data controller has a duty to protect such information and to comply with the provisions of the NDPR.

You are a data controller if you, either alone or jointly with other persons, determine how personal data is processed or will be processed.[3] Any action, such as collection, recording, organisation, storage, adaptation, alteration, retrieval, use, disclosure or dissemination[4], carried out using an individual's personal information is regarded as processing.

Furthermore, the NDPR provides that all data subjects have certain rights that protects them and limits the ability of data controllers to send repeated and random emails without the consent of the data subjects.

These rights include:
a) the right to consent to data collection[5];
b) the right to understand how and why that data is being used[6]; and
c)the right to request the deletion of that data[7].

The DPIF then provides that where there has been a breach of data of the data subjects, data controllers must provide timely reporting of such data breach to the consumers concerned[8] and to NITDA. The DPIF stipulates that such notification should be made within 72 hours[9]. Similarly, the NDPR and DPIF provides that data controllers have an obligation to conduct a full accounting of personal data that may have been compromised[10].

In practice, a data controller may engage the services of a third-party company to assist in processing personal data. For example, a telecommunication company collects data of its users manually and obtains the services of another organisation to convert the data to digital data and carry out data analytics. The latter party will be referred to as a third -party company.

[3] Section 1.3 of the NITDA Data Protection Regulation
[4] Section 1.3 of the NITDA Data Protection Regulation
[5] Article 2.3.2 of the NDPR
[6] Article 3.1.1 of the NDPR
[7] Article 3.1.7(h) & Article 3.1.9 of the NDPR
[8]Article 9.3(g) of the Data Protection Implementation Framework
[9] Article 9.3 of the Data Protection Implementation Framework
10Protection Implementation Framework

Where there is a data breach, the telecommunication company as the data controller will still be responsible for the actions or inactions of any third-party data processor it works with.

Implication of the NDPR on cold emailing

The implication of the NDPR on cold emailing is that data controllers have to take active responsibility for the data they have obtained from data subjects. They must show that they obtained consent to process this data and have processed such data for the purpose for which the data has been collected. A very common method of proving consent is through the subscription process.

Subscription processes may include a double opt-in and easy opt-out feature, and it excludes involuntary opt-ins. The opt-in feature means that a user will take an affirmative action to offer their consent. [11]The most common way through which opt-in is implemented is through checkboxes.

A data subject will be required to check a box to signify that consent has been given. Opting out, on the other hand, refers to an action where a data subject takes action to withdraw his consent[12] by either clicking an unsubscribe button or unticking a consent box.

The benefit of this approach is that data controllers can confirm that data subjects are interested in receiving emails. This enables the data controllers to weed out any fraudulent or accidental requests. This promotes more organic engagement of data subjects who receive the promotional email and may also increase the organisation's business sales. The double opt-in requirement acts as a safety net for any business sending promotional emails. Anyone subscribing to a data controller's emails should be able to do so freely and not feel compelled to do so for a particular product or service.

However, any organisation that intends to send promotional emailing to data subjects and sends such emails to 2000 people must carry out an annual full information audit[13] and review the existing data available to them[14].

[11] Termly, Opt in v. Opt out accessed on 7 October, 2020 via https://termly.io/resources/articles/opt-in-vs-opt-out/
[12] Termly, Opt in v. Opt out accessed on 7 October, 2020 via https://termly.io/resources/articles/opt-in-vs-opt-out/
13] Article 4.1.7 of the NDPR
[14] Article 4.1.5(d) of the NDPR

Where a data controller has been sending cold emails to data subjects through methods that are noncompliant with the NDPR, it is advised that it should desist from reaching out to such data subjects unless they have double-opted into such communications or the controller is sure that the consent it received cannot be disputed.

As a data controller of an organisation, obtaining double opt-in consent of its proposed clientele is essential because it increases in click-through rates and engagement it receives on its platforms, mostly as digital marketing works best when the audience a data controller intends to interact with is interested in the products and services being offered. As a data controller, your platform's engagement may allow your organisation carry out analytics on the data and decipher what the proposed clientele has an interest in.

Breach of data privacy

Similarly, an organisation that is found to be in breach of the data privacy rights of any data subject shall be liable, in addition to any other criminal liability, to either the payment of a fine of 1% of the annual gross revenue of the preceding year or payment of the sum of two million Naira (N2,000,000), whichever is greater where the data controller deals with less than 10,000 data subjects or payment of fine of 2% of the annual gross revenue of the preceding year or payment of the sum of ten million Naira (10,000,000) , whichever is greater where the data controller deals with more than 10,000 (ten thousand) data subjects.

CONCLUSION

With the developments in the data protection regulations, more organisations have been more creative in sending personalised emails. This typically increases customer engagement as data subjects appreciate the personal touch in their interaction with brands and organisations. This is an evolved or more developed cold emailing technique that has received more reception from data subjects.

However, notwithstanding the issuance of the NDPR, cold emailing and promotional emails are still being used by organisations for advertisement.

Consequently, it is advised that such promotional emails be sent with more caution and be compliant with the NDPR. The organisation must remain mindful of the rights of data subjects, particularly their right to privacy. Where in doubt on the method of compliance, reach out to a data protection compliance organisation[15] (DPCO) for guidance.

[15] AELEX is a DPCO.

ÆLEX

Opeyemi
Adeleke
(Associate, AELEX)

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana. A profile of our firm can be viewed here. You can also visit our website at www.aelex.com to learn more about our firm and its services.'

CONTACT DETAILS

LAGOS, NIGERIA

7th Floor,
Marble House
1, Kingsway Road, Falomo
P. O. Box 52901, Ikoyi
Lagos, Nigeria

Telephone: (+ 234 1) 2793367; 2793368
4736296, 4617321-3;
Facsimile: (+ 234 1) 2692072; 4617092
E-mail: lagos@aelex.com

PORT HARCOURT, NIGERIA

2nd Floor,
Right Wing UPDC Building
26, Aba Road
P.O. Box 12636, Port Harcourt
Rivers State, Nigeria

Telephone: (+234 84) 464514, 464515
574628, 574636
Facsimile: (+234 84) 464516, 574628
E-mail: portharcourt@aelex.com

ABUJA, NIGERIA

4th Floor,
Adamawa Plaza
1st Avenue, Off Shehu Shagari Way
Central Business Area
FCT Abuja, Nigeria

Telephone: (+234 9) 8704187, 6723568,
07098808416
Facsimile: (+234 9) 5230276
E-mail: abuja@aelex.com

ACCRA, GHANA

7th Floor, Suite B701
The Octagon
Accra Central, Accra
P.M.B 72, Cantonment Accra, Ghana

Telephone: (+233-302) 224828, 224845-6
Facsimile: (+233-302) 224824
E-mail: accra@aelex.com