DATA PRIVACY CHECKLIST FOR WORKING REMOTELY IN THE WAKE OF COVID-19

ARTICLE SERIES

ÆLEX

APRIL 2020

www.aelex.com

INTRODUCTION

Due to the coronavirus pandemic, employers and employees have had to work remotely in a manner that can best be described as unprecedented. We have therefore compiled a data privacy checklist that should be considered that could aid in minimising risks when working from home ("WFH").

1 DATA BREACHES

As more employees are constrained to WFH, the risk of data breaches has increased substantially. For instance, when employees are working remotely, they are prone to distractions on many fronts and may relax on cyber diligence. This could result in third parties being inadvertently exposed to official communications and information. There has also been a huge increase in cyberattacks from phishing emails to system takeovers.

Employees should be aware of the need to maintain high data protection standards when WFH and immediately report to their IT department where there is any suspicion of a data breach.

To reduce incidences of data breach, companies may provide working tools such as laptops or other relevant devices to ensure that employees limit sign in from unauthorized or insecure device.

2 SHARING OF PERSONAL DATA

Due to the coronavirus pandemic, employees may inadvertently be sharing sensitive personal data with service providers and vendors.

Under these circumstances, the employee should undertake due diligence prior to sharing such personal data and check that appropriate security measures are in place. One easy way an employee can go about this is to regularly check whether the site being accessed is secured or encrypted. This can be confirmed if the website has a padlock sign.

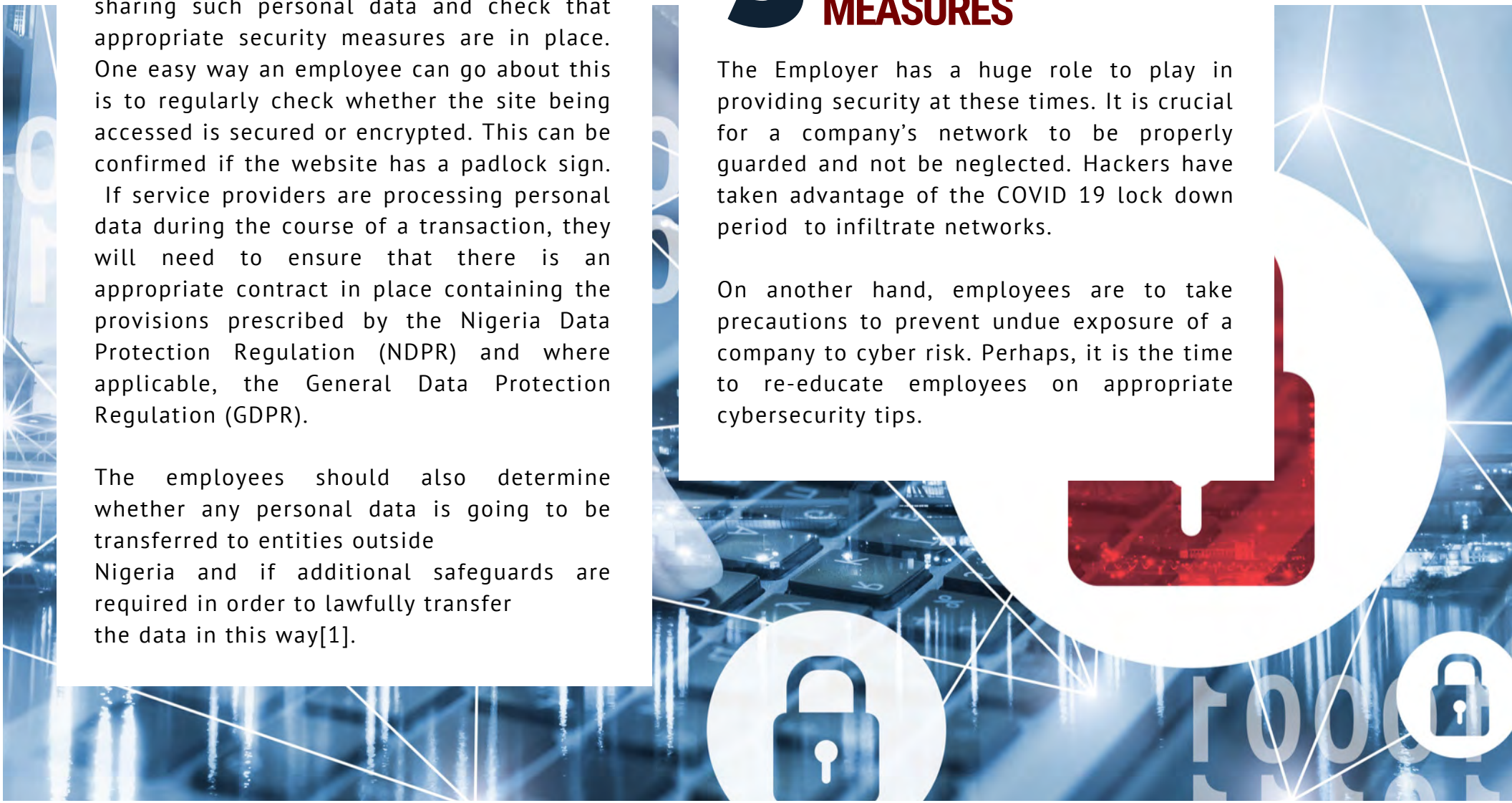
If service providers are processing personal data during the course of a transaction, they will need to ensure that there is an appropriate contract in place containing the provisions prescribed by the Nigeria Data Protection Regulation (NDPR) and where applicable, the General Data Protection Regulation (GDPR).

The employees should also determine whether any personal data is going to be transferred to entities outside Nigeria and if additional safeguards are required in order to lawfully transfer the data in this way[1].

3 SECURITY MEASURES

The Employer has a huge role to play in providing security at these times. It is crucial for a company's network to be properly guarded and not be neglected. Hackers have taken advantage of the COVID 19 lock down period to infiltrate networks.

On another hand, employees are to take precautions to prevent undue exposure of a company to cyber risk. Perhaps, it is the time to re-educate employees on appropriate cybersecurity tips.

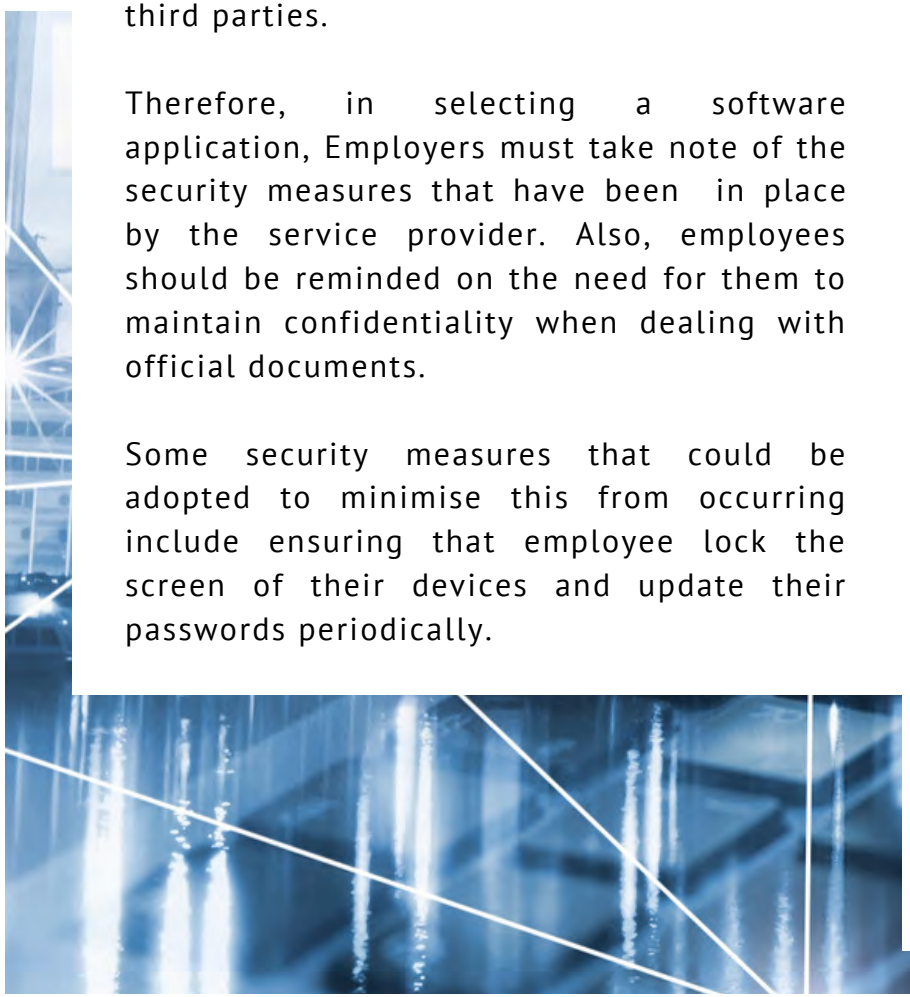


[1] Section 2.11 of the NDPR

The abrupt change in a company's operation may lead to the use of new technology. The adoption may lead to situations such as virtual meetings being hacked and sensitive conversations being overheard or leaked to third parties.

Therefore, in selecting a software application, Employers must take note of the security measures that have been in place by the service provider. Also, employees should be reminded on the need for them to maintain confidentiality when dealing with official documents.

Some security measures that could be adopted to minimise this from occurring include ensuring that employee lock the screen of their devices and update their passwords periodically.



4 USE OF PERSONAL DEVICES AND THE INTERNET OF THINGS

Not all employers are able to provide laptops and similar devices to their employees which could aid them to work remotely. Consequently, a number of employers have permitted their employees to use their personal devices in executing official instructions.

The danger behind this approach is that the personal devices of the employees may have malware that could affect the company's network. The employees could also use their personal devices to record sensitive information. Furthermore, with the Internet of Things and the connectivity of different devices, information can be circulated through different platforms that could harm the company's business eventually.

Employers may therefore need to reconsider this approach and take some security measures to limit their risk of exposure.

5 DISCLOSURE OF MEDICAL INFORMATION

Employers are required to exercise care when collecting, using and disseminating COVID-19 related information about their employees. They should therefore exercise care in balancing between providing information in the public interests and protecting individual's rights by not collecting or providing more information than is necessary. Policies should also be updated to cover self-isolation and lockdown measures.

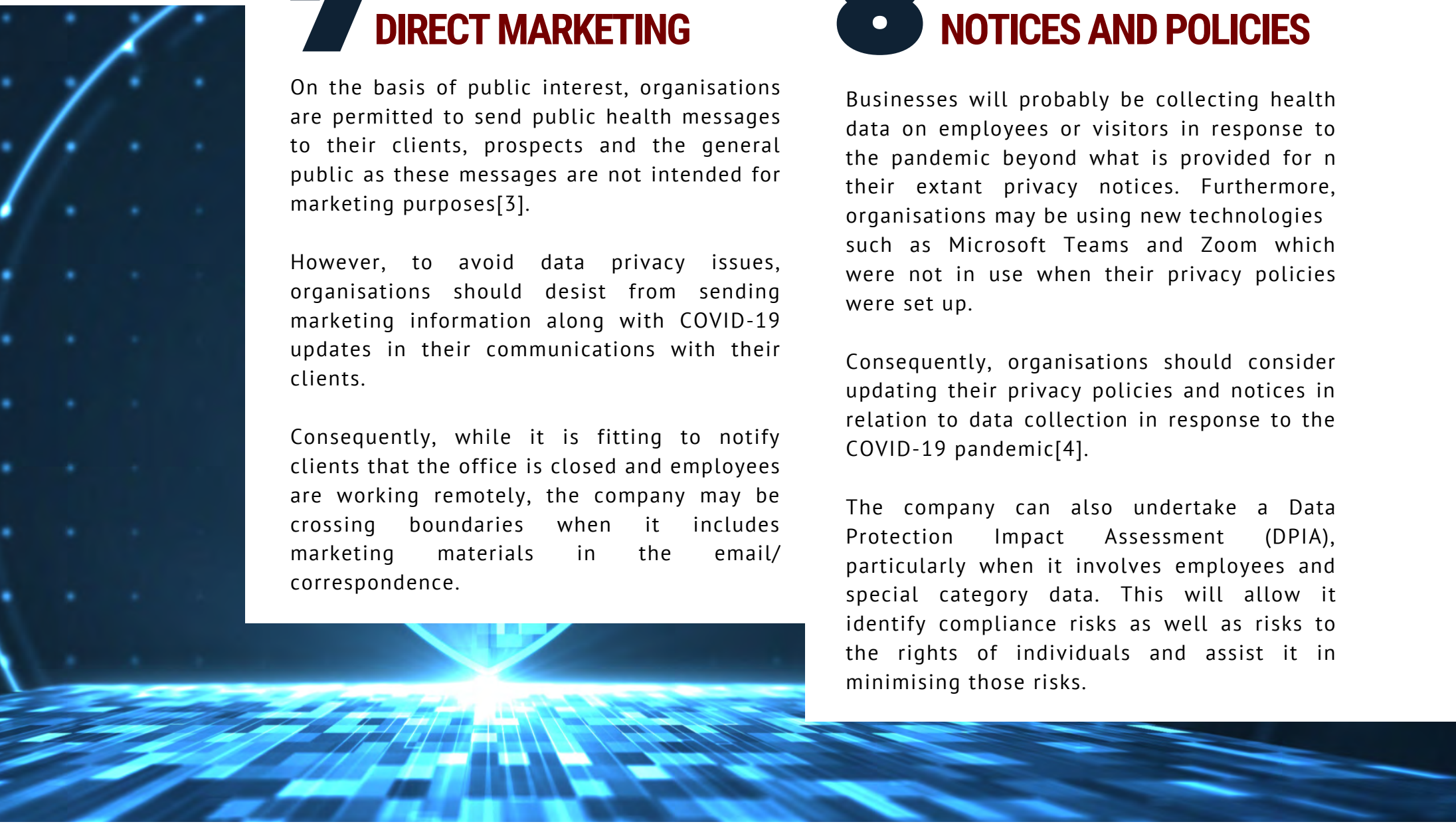
6 MONITORING EMPLOYEES

There are now several instances of different governments around the world using technology to track people to help prevent the spread of the virus. However, this has led to significant discrimination and should be approached with caution.

Most employers are also concerned that their employees may not be working remotely and may consider taking steps to monitor the activities of their employee. However, employers should be wary of using work equipment such as phones and laptops to track their employees without a legal obligation to do so.

It is therefore advisable that the employer considers this very carefully as it may be deemed as a breach of the employee's constitutional right to privacy[2]. Consequently, the employer should contact with a professional to assist it in identifying any data protection risks that may arise from monitoring employees from home.

[2] Section 37, Constitution of the Federal Republic of Nigeria (as Amended)



7 DESISTING FROM SUBTLE DIRECT MARKETING

On the basis of public interest, organisations are permitted to send public health messages to their clients, prospects and the general public as these messages are not intended for marketing purposes[3].

However, to avoid data privacy issues, organisations should desist from sending marketing information along with COVID-19 updates in their communications with their clients.

Consequently, while it is fitting to notify clients that the office is closed and employees are working remotely, the company may be crossing boundaries when it includes marketing materials in the email/ correspondence.

8 UPDATING PRIVACY NOTICES AND POLICIES

Businesses will probably be collecting health data on employees or visitors in response to the pandemic beyond what is provided for n their extant privacy notices. Furthermore, organisations may be using new technologies such as Microsoft Teams and Zoom which were not in use when their privacy policies were set up.

Consequently, organisations should consider updating their privacy policies and notices in relation to data collection in response to the COVID-19 pandemic[4].

The company can also undertake a Data Protection Impact Assessment (DPIA), particularly when it involves employees and special category data. This will allow it identify compliance risks as well as risks to the rights of individuals and assist it in minimising those risks.

{3] Section 2.2 of the NDPR
[4] Section 2.5 of the NDPR

ÆLEX

Davidson Oturu
PARTNER

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 us at:

4th Floor, Marble House,
1 Kingsway Road, Falomo Ikoyi,
Lagos, Nigeria

Telephone: (+234-1) 4617321-3, 2793367-8, 7406533,

E-mail: lagos@aelex.com

Click here www.aelex.com

to follow our social media handles click below

@aelexpartners