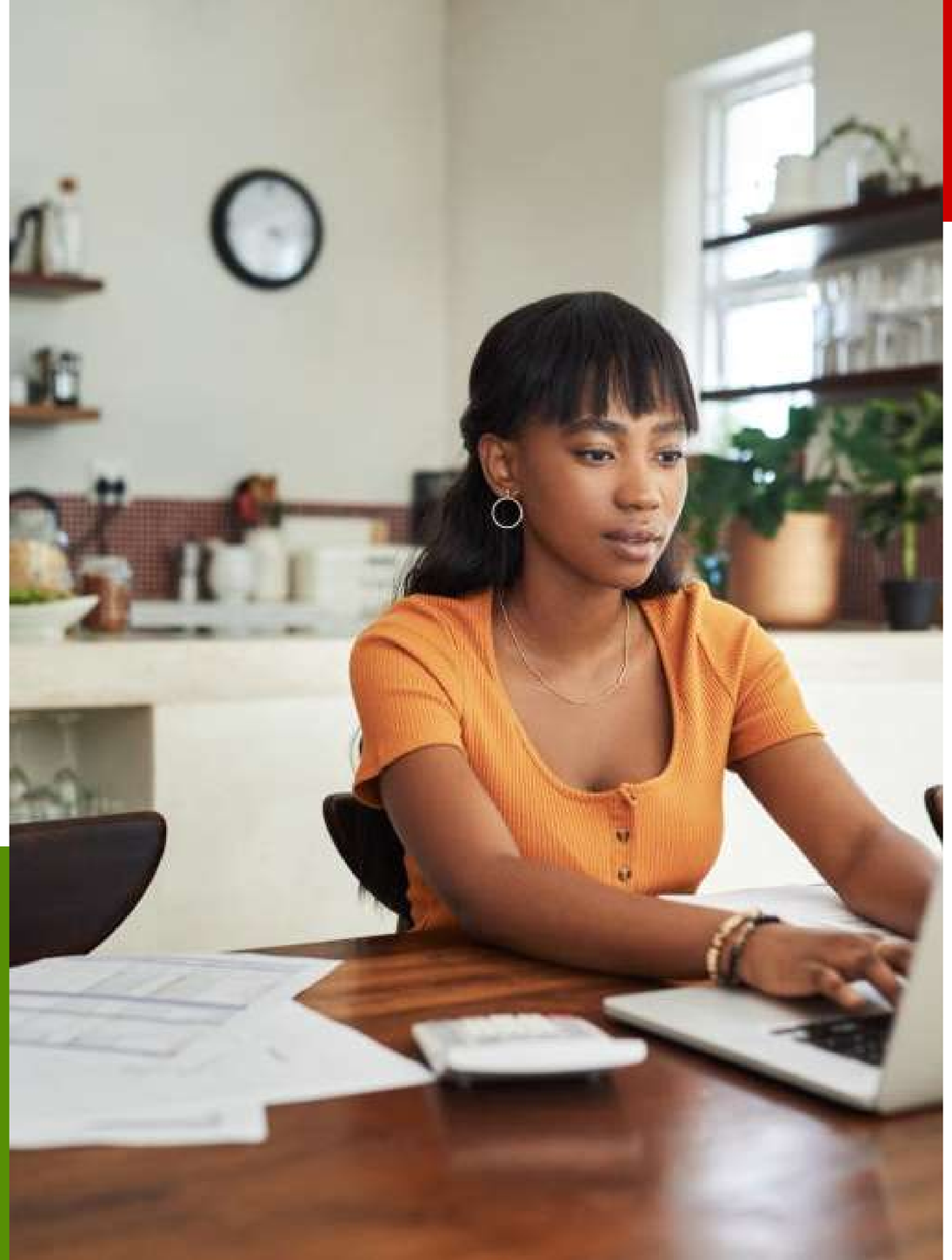
COVID 19 - Remote Working & Data Protection - Risk Mitigation Strategies



Introduction:

With the effect of the Corona Virus Disease (“Covid-19”), Organizations all around the world have compulsorily had to migrate their daily business activities and transactions to remote work platforms. Ordinarily, an organization would test such a system before implementation but the sudden spring of Covid-19 has made many organizations adopt the pattern without any proper planning and test implementation. Proper planning would include proper staff training on the use of specified virtual offices and data protection, implementation of proper cybersecurity systems, introduction to modified documents access, such as the Microsoft sharepoint, etc.

In Nigeria, where the concept of virtual offices is bourgeoning, technology has become more essential than ever in light of the pandemic as the lockdown rules and social distancing measures have forced the implementation of stay-at-home orders.

Introduction:

Very importantly, remote working presents its own unique data and cybersecurity challenges. All risks associated with remote working have the capacity to impact an organization's compliance with Data Protection and Privacy Regulations. This briefing note focuses on highlighting key issues arising from the adoption of remote working and measures that can be taken to ensure security of personal data while working
remotely.

Key Issues/Risk Mitigation Strategies:

Taxtech AO2LAW

1. Training and Staff Awareness

As required by the Nigeria Data Protection Regulation ("NDPR" or the "Regulations"), all persons entrusted with Personal Data of a Data Subject or who are in possession of the Personal Data of a Data Subject owe a duty of care to the said Data Subject. [1] Therecent case of WM Morrison Supermarkets Plc v. Various Claimants (2020) UKSC 12 (the "Morrison case") underscores the importance of ensuring that an organization's staff deals properly with whatever personal information a Data Subject has entrusted to the organization. In that case, an embittered employee published the personal information of 98,998 employees of Morrison Supermarkets on a public website, thereby exposing the personal information of these employees. The aggrieved employees brought an action for vicarious liability against Morrison. The trial courts and appeal courts held that Morrison was vicariously liable for the conduct of the embittered employee.

Ultimately, the UK Supreme Court held that the employee's conduct was not so closely connected with acts which he was authorized to do that it can fairly and properly be regarded as done by him while acting in the ordinary course of his employment. Organizations are therefore encouraged to ensure employees/staff put in place best data protection practices to ensure compliance with the Regulations and avoid the risk of suits from aggrieved Data Subjects.

2. Review of Internal Policies

The NDPR requires that for any medium through which Personal Data is being collected or processed, a simple and conspicuous privacy policy that the class of Data Subject being targeted understands must be displayed. At this time when organizations have migrated virtually, it has now become important to ensure privacy policies and other internal policies such as: policy on email use, policy on password protection, policy on confidential information, policy on access control, policy on information transfer, communication security and teleworking, among others are duly observed by employees/staff. Flowing from this, it is recommended that organizations must ensure that internal Data Protection policies are either put in place or reviewed and revised to ensure efficiency in remote work environments.

3. System Protection

As a consequence of remote working, new work setups will come with many new challenges, including the protection of Sensitive Personal Data. Without the security protections that come with being in the office, such as IP addresses, Local Area Network (LAN), and WIFI, the organization becomes exposed to an array of security vulnerabilities such as hacking, phishing, malware, not to mention employees not given to the remote working system. Information security must therefore be a top priority during this time.

Organisations are therefore advised to put in place certain security features such as firewalls (e.g. proxy firewalls, packet-filtering firewalls, stateful inspection firewalls, hardware firewalls, software firewalls), anti-virus, and endpoint protections on all assets given to employees. In the event of phishing, there are several steps a Data Controller may take to mitigate and eventually stop these phishing activities. A Data Controller may carry out a Vulnerability Assessment Test in order to detect any vulnerabilities in its system especially with regards to security of its data base.This is to ensure that there is no flaw in its data processing activities which may lead to a breach of personal data. Where a flaw is discovered, steps should be taken to fix such flaws. Furthermore, a Data Controller may contact data subjects who receive phishing emails or phone calls and communicate measures to be taken to disrupt these phishing activities in order to reduce the risk of a data breach and mitigate the impact in the event that a breach has already occurred.

4. Data Transfer Pseudonymization and Encryption

It is recommended that where Personal Data is to be transferred from one location to another, it should be pseudonymised or encrypted to protect it, in the event it is intercepted during the transfer.

Pseudonymisation is the processing of Personal Data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

Encryption refers to the procedure that converts clear text into a hashed code using a key, where the outgoing information only becomes readable again by using the correct key. While, pseudonymisation allows anyone with access to the data to view part of the data set, encryption allows only approved users to access the full data set.

Organisations are therefore advised to encrypt or pseudonymize Personal Data during transfer using encrypting applications. Please note that encryption can pseudonymization can be done for remote working arrangements as well. There are off the shelf applications that do this and can be easily purchased.

5. Technology Solutions

A number of technology solutions may be considered to help secure remote working:

(a) **Voice over Internet Protocol, VoIP:** VoIP has become ubiquitous and thus cuts communication costs, keeping the team's virtual connectivity alive at the same time. Teleconference tools keep the communication channel open with clients and co-workers, meetings schedule, webinars, presentations, instant messaging;

(b) **VPN**: A virtual private network (VPN) is a network that is constructed using public wires usually the internet to connect remote users or regional offices to a company's private, internal network. Putting this in place will make it possible for employees to connect to the office resources from the comfort of their homes. VPN provides a secure communication channel through public Internet connections to existing private network in the office;

(c) **Malware Protection:** Default firewall and antivirus protection that comes with most PCs is not enough. Anti-malwares should be installed on all devices both personal and official used to process Personal Data. Constant update and upgrade is also necessary to drive efficient business security solutions. It is necessary that every Sensitive Personal Data sits behind a firewall (an intrusion detection system) at the very least;

(d) **Password Combinations:** Organisations need to ensure tighter password credentials for internet routers used by staff outside the office;

(e) **Network Security:** Network security in an organization is paramount. The IT team needs to ensure that the core organisation infrastructure sits behind a firewall;

(f) **Data Backup/Recovery:** It is essential to make sure employees working remotely have access to backup solutions to prevent data loss. Dual backup of primary and secondary storage locations could go on cloud and on-premise location at the same time to avoid downtime. Do ensure you review organisation's policies with them to ensure they are always backing up. There are a host of cloud infrastructure online that can be subscribed to.

Conclusion

In order to stay secure and also ensure compliance, it is recommended that Data Controllers and Administrators regularly consult their Data Protection Officers, Data Protection Compliance Organizations as well as the Regulation – to ensure full compliance and protection of information.

This briefing note has been put together by Taxaide Technologies Limited and AO2LAW. For further information on the foregoing (none of which should be taken as legal advice), please contact:

Chiedu Mokwunye (c.mokwunye@taxaide.com.ng)
Uwemedimo Atakpo (u.atakpo@taxaide.com.ng)
Kitan Kola – Adefemi (kitan.kola-adefemi@ao2law.com)
Oyeyemi Oke (Oyeyemi.oke@ao2law.com)