G. ELIAS & CO. | ALN

THE LAW ON DEPLOYING DLP SOFTWARE TO MONITOR EMPLOYEE ONLINE ACTIVITIES

THE LAW ON DEPLOYING DLP SOFTWARE TO MONITOR EMPLOYEE ONLINE ACTIVITIES

This article explores how data loss prevention (DLP) software may be deployed by organizations to protect their data and information and the legal implications of the use of DLP software with respect to the rights of the organization's employees and External Parties. DLP software protects corporate information; provides reporting information to meet compliance and auditing requirements (*e.g.* the requirement of the Nigerian Data Protection Regulations on data protection audits); protects the intellectual property and trade secrets of the organization; and ensures data visibility.

These are vital issues that are necessary to protect the business of organizations. Below we look at: (i) the background to the use of DLP software; (ii) implementation of DLP software; (iii) possible infringement of privacy rights; (iv) compliance with the NDPR, and (v) how employers can monitor employee online activities within the purview of the law.

Background to the Use of DLP software

Since the advent of information technology, organizations have leveraged on various technologies to enhance the performance of employees and their overall performance. Conventionally, organizations possess networks, central servers, applications, databases, mobile applications, cloud services, SharePoint sites, e-mail, calendar, contacts and other information (**IT Assets**) used in connection with the organization's business. These IT Assets can be accessed by employees either with a device owned by the employee (**Personal Device**) or a device provided by the organization to the employee for carrying out his duties as an employee (**Official Device**). An organization's IT Assets can also be accessed by persons who, though not employees of the organization, require temporary access for various reasons (**External Party(ies)**). A good example is where an External Party temporarily accesses the wifi network of an organization.

Understandably, an organization's IT Assets contain sensitive information, including trade secrets and confidential information of the organization and clients of the organization that need to be protected. There is a risk of such confidential information being accessed, used or transferred without authorization by not only employees but even External Parties who use the organization's IT Assets. The unauthorized use of confidential information can be detrimental to the business of any organization and expose an organization to liability for claims by third parties who have suffered damage resulting from the unauthorized use of such confidential information. The obvious risks to an organization's sensitive information have compelled organizations to monitor the online activities of employees. The disruption caused by the COVID- 19 pandemic and the consequent requirement for employees to work remotely has served to further heighten the need for organizations to monitor the online activities of employees.

The tools, solutions and software that ensure that the sensitive and confidential information of an organization is not accessed without authorization, deleted, maliciously transferred or misused in general consitute DLP software. DLP software is used to monitor employee and External Parties' online activities to ensure that an organization has reasonable control and visibility over the use of its IT Assets.

Implementation of DLP Software

Organizations can implement DLP software by installing and administering the same on Official Devices, Personal Devices and devices belonging to External Parties.

An organization can install DLP software to monitor the activities of an employee when using an Official Device, such as computers and mobile phones. The DLP software monitors and controls end-point activities, filters data streams on corporate networks and monitors data in the cloud to protect data at rest, in motion and in use. The organization using DLP software can access and monitor browsing history, key stroke activity, files saved on the Official Device, and the e-mails sent with and received on the Official Device. The organization can also remotely access and control such Official Devices. Ideally, an employee should use an Official device for only official purposes. However, the reality is most employees use Official devices for personal purposes as well. The result is that the organization in fact has access to personal information stored or transmitted through the Official device and can monitor personal activities carried out with the Official Device.

An organization can deploy DLP software in Personal Devices that are used to access the organization's IT Assets. Some employees find it more convenient to access the organization's IT Assets with just one device – preferably their Personal device, instead of managing both a Personal device and an Official Device. The use of a Personal Device that can access an organization's IT Assets also makes it convenient for an employee to work from anywhere at any time. The deployment of DLP software in Personal Devices is usually accompanied with the installation of a mobile device management (**MDM**) software. The MDM software separates official information/activities from personal information/activities carried out on the Personal Device. The installation of the MDM software also gives the organization access to the personal information (such as text messages, browsing history, the location of the employee in real time) transmitted through or with the Personal Device. The access to personal information on the Personal Device of the employee whether inadvertent or intentional exposes the organization to privacy-related legal risks.

DLP software can also be used to monitor the access of devices owned by External Parties, to the organization's IT Asset. This scenario most often plays out where the device of the External Party accesses the wi-fi network of the organization. By connecting to this network, the organization has a level of control and access to the device of the External Party for the period the device is connected to the organization's network. During this period the organization may have access to the External Party's personal information, and this also has legal implications.

Possible Infringement of Privacy Rights of Employees and External Parties

It is re-iterated that where an organization uses DLP software to monitor the Personal Device or Official Device of its employees or the device of an External Party, the organization has access to the personal information of such employee or External Party. Access to such personal information is usually a breach of the employee's right to privacy.

The right to privacy of every citizen including employees is constitutionally protected. Section 37 of the Constitution of the Federal Republic of Nigeria as amended provides that:

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

Nigerian courts have in several cases recognised the constitutional right to privacy. See *FRN v. Daniel* (2011) LPELR-4152 (CA); *Okafor v. Ntoka* (2017) LPELR-42794 (CA), where the Court of Appeal judicially acknowledged the right to privacy, albeit in the context of the right to privacy being subject to certain exceptions.

In practice employees execute agreements or sign forms that evidence their consent to the use of DLP software by organizations to monitor their online activities. These agreements or forms usually inform the employee of the possibility of the organization accessing the employee's personal and private information. In our opinion, the legal effect of the execution of such an agreement by the employee, consenting to the possible infringement of his privacy amounts to a waiver of the employee's right to privacy. Appreciating the fact that the employee may execute a document that has the effect of a waiver of his right to privacy, the pertinent issue is, can a fundamental right be waived?

Fundamental rights are generally inalienable. The only constitutionally recognized limitation on the right to privacy is by way of a law that is reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality or public health or for the purpose of protecting the rights and freedom of the other persons (Section 45 of the Constitution, *Okafor v. Ntoka, supra*).

However as an exception to the general rule of the inalienability and non-waiver of constitutionally provided rights, the courts have held that a person can waive a constitutionally vested right, provided that the person enjoys the sole benefit that accrue by virtue of this right (*Ariori v. Elemo (1983) LPELR-552 (SC) and NNPC v. Nwodo (2018) LPELR45872 (CA)*).

In *Ariori v. Elomo* (1983) supra, the Supreme Court held as follows:

> *"…**When a right is conferred solely for the benefit of an individual there should be no problem as to the extent to which he could waive such right. The right is for his benefit. He is sui generis. He is under no legal disability. He should be able to forego the right or in other words waive it either completely or partially, depending on his free choice. The extent to which he has foregone his right would be a matter of fact and each case will depend on its peculiar facts.** A simple example could be seen in a right which has been conferred by contract, whereby the benefit is principally for him, he has full competence to waive that right. What obtains in the case of a contract should go for benefits conferred by statute. A beneficiary under statute should have full competence to waive those rights once the rights are solely for his benefit. The only exception I can think of is where the statute itself forbids waiver of its statutory provisions."* (Emphasis supplied.)

Further, in *Pam v. ANPP* (2008) 4 NWLR (Pt. 1077) 219 at 250G–H, the court held that

> *""Where the law makes provision in favour of a person, such a person can waive his right under the law. **Even where the provisions involve the fundamental rights of the***

> ***person concerned, he can in appropriate circumstances, waive the rights. Thus, if the beneficiary of the statutory provisions waives his rights, or is deemed to have waived them, he cannot be heard later to complain about the violation of those rights."*** (Emphasis supplied.)

Thus, by the authority of the cases cited above, an employee can validly waive his right to privacy where he is the sole beneficiary of such right and all protections afforded by the existence of such right are enjoyed solely by the employee. This also means that there should be no considerations with respect to public interest or the right of a third party that will prevent the employee from waiving this right by giving consent to access his personal information.

Note that the waiver granted by the employee does not absolve the organization of its duty to keep such personal information confidential, especially where the organization has contracted with the employee to keep such private information confidential. This duty of care extends to the transfer of such personal information to third parties. The organization must ensure that where such personal information is transferred to third parties such third parties equally undertake to keep the personal information of the employee confidential.

Compliance with the NDPR

Another legal implication of monitoring an employee's use of corporate, personal and external third party devices, including accessing, decrypting and inspecting encrypted internet traffic, using and disclosing information that may be stored on such devices, will require the organization to comply with the processing requirements of the Nigerian Data Protection Regulation (**NDPR**) 2019.

The NDPR stipulates standards that are required to be observed by any organization that processes the personal data of data subjects (employees). These standards impose a duty of care that an organization must adhere to. Organizations are obligated to collect and process data of employees in accordance with the NDPR 2019. In particular, organizations should ensure that the personal data of employees are: (i) collected and processed in accordance with specific, legitimate and lawful purposes consented to by the employee; (ii) adequate, accurate and without prejudice to the dignity of the human person; (iii) stored only for the period within which it is reasonably needed to be stored, and (iv) secured against all reasonably foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements.

Further, the organization in the course of processing the personal data of the employee or External Parties must ensure that such processing is lawful as provided by the NDPR. To comply with the provisions of the NDPR, the organization should process the personal data of the employee or an External Party: (i) with the consent of the employee or the External Party; (ii) in relation to the performance of a contract to which the employee or the External Party is a party; (iii) in compliance with legal obligations imposed on the organization; (iv) for the protection of the vital interests of the employee or the External Party; and (v) for the performance of a task carried out in the public interest or in the exercise of an official public mandate vested in the organization.

Where data is to be processed by a third party on behalf of or in conjunction with the organization, the third party must execute a written contract, wherein the third party will undertake to adhere to the provisions of the NDPR in processing the data of employees. The duty of care in processing the data of employees and External Parties remains on the organization whether the processing of the data is in fact done by a third party or not.

Also, where the personal data of the employee is transferred to a foreign country or a foreign entity, the organization must ensure that the foreign country or entity abides by similar or higher standards of data protection, comparable to the standards provided for by the NDPR.

How Organizations can Monitor Employees within the Purview of the Law

Having discussed the legal implications of monitoring employees and External parties, how can organizations ensure that they remain within the ambit of the law in the deployment of DLP software?

a. Employees must agree to the Implementation of DLP Software

Organizations should ensure that employees accept the terms and conditions upon which the DLP software will be implemented. These terms and conditions could be in the form of a user agreement or an acknowledgment form or even a click wrap agreement, which employees will be required to execute before the implementation of the use of DLP software. The user agreement should clearly: (i) provide for obtaining the consent of the employee for the installation of the DLP software on the employee's Personal Device or Official Device; (ii) explain the purpose of the installation of the DLP software; (iii) state the nature and extent of the organization's access to information and content, both personal and official, in the employee's Personal Device or Official Device; and (iv) place an obligation on the organization to keep confidential, personal information obtained for the purpose of the installation of the DLP software or as a consequence of the administration of the DLP software. This obligation should also be contractually extended to third parties who process such data on behalf of the organization. The Agreement could also reference any relevant policies issued by the organization in line with the below.

b. Clear Monitoring Policy

The organization should issue a clear policy on the monitoring of Personal Devices and Official Devices of employees and a privacy policy on its data protection practices. The policy on monitoring should state particulars such as who is being monitored, what is being monitored (internet usage, electronic communications, keystroke logging, real time location and so forth), the scope of the monitoring activities and modalities for the restriction of access to unauthorised content or a requirement of additional clearance before accessing particular content. Generally, organizations should ensure that they have adequate security measures installed for the protection of the personal information of employees against cyber-attacks and other similar dangers.

The NDPR requires the issuance of a simple and conspicuous privacy policy on any medium through which personal data is collected and processed. Organizations can display this privacy policy on their websites or on forms used to collect the personal data of employees. The privacy policy must contain the relevant information stipulated in the NDPR, which include what constitutes consent, description of the personal information to be collected, and the purpose for the collection of personal data.

c. Click Wrap Agreements

The organization can use click wrap agreements, especially for External Parties who access the organization's IT assets temporarily. The External Party should be required to accept the terms of the click wrap agreement before accessing the organization's IT assets. The click wrap agreement should also include links to the more exhaustive statements of the terms and conditions and other relevant policies.

Conclusion

We re-iterate that DLP software protects corporate information, provides reporting to meet compliance and auditing requirements, (*e.g.* the requirement of the NDPR on data protection audits), protects the intellectual property and trade secrets of the organization and ensures data visibility. Organizations should ensure that they appreciate the legal implications of deploying DLP software and ensure that their use and administration of DLP software is in compliance with relevant laws and in line with best practice on data protection and privacy.

Authors

Ebimobowei Jikenghan
Senior Associate
ebi.jikenghan@gelias.com

Novo Edojariogba
Associate
novo.edojariogba@gelias.com

This publication does not constitute legal advice and does not create a client-attorney relationship. For assistance with any legal issues that may arise on implementation of DLP software, monitoring policies, privacy rights and data protection, please contact us at neweconomy@gelias.com

G. ELIAS & CO.

LAGOS OFFICE

6, Broad Street
Lagos
Nigeria

T: +234 (1) 460 7890;
280 6970
E: gelias@gelias.com

ABUJA OFFICE

2nd Floor, Abia House
Plot 979, First Avenue
Central Business District
Federal Capital Territory
Abuja

T: +234 (1) 888 8881

www.gelias.com