UUBO COVID-19
RESOURCE HUB:

ANSWERS TO YOUR QUESTIONS ON PERSONAL DATA PROTECTION AND SECURITY

UDO UDOMA & BELO-OSAGIE

Introduction

As the incidents of the Covid-19 pandemic began to increase in Nigeria, the Federal Government of Nigeria directed that all businesses in Lagos State, and the Federal Capital Territory, Abuja, the worst hit locations, and also Ogun State because of its proximity to Lagos State, which are not exempted in the COVID-19 Regulation, 2019 to shut down for an initial period of 14 days, starting from 11pm on Monday, 30th March 2020. Several states across the country have also implemented varying degrees of quarantine measures, including the restriction of movement, all aimed at containing the spread of the virus.

In this update, we aim to provide some highlights, in the form of questions and answers, to assist your organisation to remain compliant with its data protection obligations while complying with the directives of the Federal and state governments in connection with the fight against the COVID-19 pandemic.

1 Can we still file our data protection report with the National Information Technology Development Agency?

If you missed the statutory deadline (15th March) for filing your data protection audit report, you have up to 15th May 2020 to file your data protection audit report with the National Information Technology Development Agency (the "**NITDA**"), provided you engage the service of a Data Protection Compliance Organisation ("**DPCO**") to conduct the audit, and have the DPCO apply for an extension of time to file the audit report before the deadline. Our firm is a NITDA licensed DPCO and would be happy to assist you in this regard.

2 Can we test employees for COVID-19 and disclose the identity of an employee that tested positive?

The consent of the employee will be required before an employee can be tested. You can, however, check the temperature of employees before they are allowed access to the office as a safety measure, and any personal information that is processed as a consequence of such temperature check will be lawful on the basis that it is for the protection of the vital interests of the employee and his or her colleagues and the society at large.

You have a duty to ensure that the identity of an employee who tests positive for COVID-19 is protected. The identity of the employee can be disclosed where such disclosure is required by law, for instance, a disclosure to public health authorities including the Nigeria Centre for Disease Control ("**NCDC**") and the Federal or State Ministry of Health etc. The disclosure should, however, be restricted to personal data relevant for the identification, isolation and treatment of the employee.

3 Can we process personal data without consent during the pandemic?

In the absence of the Data Subject's consent, you can only process personal data where processing is necessary for the:

1. performance of a contract to which the Data Subject is a party, or in order to take steps at the request of the Data Subject prior to entering into a contract;
2. compliance with a legal obligation to which you are subject;
3. protection of the vital interests of the Data Subject or another natural person; or
4. performance of a task carried out in the public interest or in the exercise of an official public mandate vested in you.

4 Can we transfer employees' medical information to our parent company, foreign partners, or advisers offshore?

Yes, you can transfer employee medical information to your parent company, foreign partners or advisers offshore if:

1

you obtain an adequacy decision from the NITDA that the country or international organisation you intend to transfer the data to has adequate data protection safeguards; and the transfer is done subject to the supervision of the Attorney-General of the Federation (the "AGF").
or

2

the data subject whose personal data is being transferred has explicitly:

i. been informed of the organisation's obligation to transfer the data with the AGF's supervision and that such supervision has not been sought;

ii. been informed of the possible risks of such transfers; and

iii. consented to the transfer.

or

3

the transfer is necessary for:

i. the performance of a contract between you and the Data Subject or the implementation of pre-contractual measures taken at the Data Subject's request;
ii. the conclusion or performance of a contract concluded in the interest of the Data Subject between you and another natural or legal person;
iii. important reasons of public interest;
iv. the establishment, exercise or defence of legal claims; or
v. protecting the vital interests of the Data Subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Prior to transferring personal data under paragraphs 4 (b) and (c) above, you should ensure that the Data Subject understands through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of the transfer.

5 Can we share personal data with vendors who are assisting us to set up our telecommuting infrastructure?

Yes, you can share personal data with your vendors. Prior to sharing the personal data, you should:

1. ensure that the vendor or the category of vendor has been disclosed as a third party that processes information on your behalf in your privacy policy;
2. conduct due diligence on the vendor, in order to ensure that the vendor does not have a history of data protection violation;
3. ensure that the personal data is processed with the consent of the Data Subject or under any of the heads in paragraph 3 above; and
4. execute a written contract with the vendor, and insert a provision requiring the vendor to comply with the provisions of the Nigeria Data Protection Regulation 2019, or any data protection law in the vendor's jurisdiction.

6 Will the authorities take action against us if our data protection standards do not meet the usual standard or we do not respond to information requests as quickly as usual?

The authorities may sanction you if your data protection standards fall below the recommended threshold or you do not respond to information requests as required.

If due to the lockdown or any other reason, you are unable to respond to information requests as quickly as usual, you should immediately but not later than 1 (one) month after receipt of the request, inform the Data Subject of the reason(s) for not taking action and of their right to lodge a complaint with the NITDA on the basis of your refusal. In addition to this and to avoid being penalised, it is advisable that you should immediately:

1. notify the NITDA of your inability to promptly respond to information requests; and
2. put up a notice to this effect on every medium through which you collect personal data.

7 With most of our workforce telecommuting, what are our data protection obligations in relation to remote working?

You should consider adopting a telecommuting policy to guide members of staff on their conduct, especially in relation to data protection and privacy. You should also consider providing data protection training for employees that handle personal data, if one has not been provided in recent times.

Employees should be required to abide by the organisation's data protection policy and to adopt "common sense" security measures such as restricting access to work documents and laptops, not using personal devices for work, and not disclosing personal information over an unsecure network or device etc.

8 Can we monitor employees' online presence?

Yes, you can monitor the online presence of employees during normal work hours, in order to ensure that employees are delivering on assigned tasks. You should, however, inform employees of this prior to implementation, and consider suitable alternatives for employees who are adverse to such monitoring, including having employees use a time tracking application to record the time spent on tasks or have them provide daily updates to their team leads. Such monitoring should, however, be limited to devices provided by the employer or devices that the employee expressly consents to the employer gaining remote access to.

9 Should we update our privacy policy?

It may be useful to review your privacy policy, in order to ensure that your collection and use of the personal data during the pandemic is properly documented. This review is important if you have introduced another medium of collecting data, want to process data for a new purpose, or want to share personal data with a new category of third parties etc.

9 As part of our strategy to protect our workforce from COVID-19, can we require employees to provide their medical data when they resume?

You can require employees to provide their medical data, if the:

1. contract of employment or employee handbook requires the provision of such data in this circumstance; or

2. contract of employment or employee handbook requires the provision of such data in this circumstance; or

In the absence of any of the above-mentioned circumstances, the employee needs to consent to the provision of such data. Where the employee refuses to give such consent, and you reasonably fear that the employee is infected or may infect other employees, you can require the employee to work from home or contact the NCDC or other relevant government agencies on one of their helplines.

11 How do we protect personal data in our possession

As stated in paragraph 7 above, the authorities may sanction you if your data protection standards fall below the recommended threshold. You should, therefore, continue to implement existing personal data security measures.

In addition to the commentary in paragraph 8 above, it may be useful to conduct an internal audit of your data protection practices at this time to identify security lapses and any security breach.

Conclusion

As a business, you must continue to evaluate how you collect, process and store personal data, with a view to ensuring compliance. If you are in doubt about what steps to take at this time, in order to ensure compliance with applicable data protection laws, kindly seek advice from a DPCO. As a NITDA licensed DPCO, we will be glad to assist you in this regard, if required.

This guidance note is for general information purposes only and does not constitute legal advice and does not purport to be fully comprehensive. If you have any questions or require any assistance or clarification on how the subject of this guidance note applies to your business, or require the services of a Data Protection Compliance Organisation, please contact Jumoke Lambo at jumoke.lambo@uubo.org; dp@uubo.org or uubo@uubo.org.