Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2021-009[1]

17 March 2021

[redacted]

Re: FORENSIC AUDIT ON COMPANY-ISSUED ASSETS AND COMPANY-RELATED ACCOUNTS

Dear [redacted]

We write in response to your email received by the National Privacy Commission (NPC) which sought to clarify whether the conduct of a forensic audit on company-issued assets and company-related accounts will have any negative implications or non-compliance with the Data Privacy Act of 2012[2] (DPA) and if there are any specific guidelines for such audits.

We understand that the internal audit team of your company is planning to perform a forensic audit on company-issued assets such as laptops and mobile phones, and company-related accounts and accesses such as email addresses, WiFi access, browsing and download history, among others. The purpose of such forensic audit is to ensure that no confidential company information is disclosed to third parties and that the use of company-issued assets shall not cause any type of company information breach.

The NPC has limited information as to the actual scope of the forensic audit which may involve personal and sensitive personal information (collectively, personal data) stored in the company-issued assets and accounts. Nevertheless, should the processing activity involve personal data, the same should have a lawful basis under the DPA.

Lawful basis for processing personal and sensitive personal information; general data privacy principles

[1] Tags: forensic audits; general data privacy principles; lawful basis for processing; data subject rights.
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 4 (2012). Tags: forensic audits; general data privacy principles; lawful basis lawful basis for processing;

The DPA provides for the various lawful criteria for processing personal data under Section 12 (personal information) and Section 13 (sensitive personal information). The company, as a personal information controller (PIC), should make a determination of the most appropriate lawful basis.

In any case, the company is expected to adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality, and should consider the following factors on the proposed activity:

- necessity and the lawful basis that may be applicable;
- fairness to the employees;
- proportionality of the processing to the concerns raised by the company; and
- transparency of the activity.[3]

If there are means through which the company can conduct the forensic audit without accessing and/or otherwise processing personal data contained in devices and accounts, such options should be explored and implemented.

We reiterate that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose, i.e., forensic audit. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[4]

General guidance; transparency; data subject rights; security measures

Aside from determining the lawful basis for processing, the company should inform and notify the employees of the nature, purpose, and actual method and extent of the forensic audit, security measures to protect personal data, as well as the procedure for redress in cases where the rights of the employee as a data subject are violated.[5] The company, as a PIC, is required to uphold data subject rights. For further guidance, you may refer to NPC Advisory No. 2021-01 - Data Subject Rights.

The company also has the obligation to implement reasonable and appropriate organizational, technical, and physical security measures for the protection of personal data which may be involved in the forensic audit. This may entail requiring persons who will be conducting the audit to sign non-disclosure agreements, where appropriate, to ensure confidentiality. If the company will be outsourcing the forensic audit to a third-party service provider, such arrangement must be covered by an outsourcing agreement or similar document which shall clearly identify the corresponding obligations and liabilities of the parties.

We wish to emphasize that while the employees using the company-issued assets and company-related accounts may reasonably expect that the company would conduct periodic audits on said assets and accounts to ensure the security of company information and

[3] See: European Commission, Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, adopted on 8 June 2017, page 11, *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (last accessed: 16 March 2021).
[4] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).
[5] *Id.* § 18 (a).

network, employers should keep in mind that employees are still entitled to their right to privacy at work.[6]

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

[6] See: National Privacy Commission, NPC Advisory Opinion No. 2018-084 (Nov. 28, 2018).