Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-084

28 November 2018

[redacted]

Re: COMPUTER MONITORING

Dear [redacted],

We write in response to your inquiry on whether secret surveillance on an employee's computer activities through the installation of a monitoring software to record keystrokes and take random snapshot of computer screen is prohibited under the Data Privacy Act of 2012[1] (DPA).

We wish to limit the succeeding discussion on an employer's act of monitoring the employees at the workplace, specifically, monitoring employee activities when he or she is using an office-issued computer.

Scope of the DPA; general data privacy principles

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. Where the computer monitoring results in the collection of personal, sensitive personal or privileged information (collectively, personal data) of employees, the employers are engaged in processing personal data, and thus, covered by the provisions of the DPA.

Monitoring employee activities when he or she is using an office-issued computer may be allowable under the DPA, provided the processing falls under any of the criteria for lawful processing of personal data under Sections 12 and/or 13 of the law.

Employers, as personal information controllers (PICs), shall ensure that the processing complies with the general data privacy principles of transparency, legitimate purpose and proportionality.

First, it is incumbent upon the employer to determine the purpose/s of computer monitoring, which must not be contrary to law, morals, or public policy.[2] Some possible legitimate purposes of computing monitoring are as follows: management of workplace productivity,

[1] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (b) (2016).

protection of employees, business assets, intellectual property or other proprietary rights, prevention of vicarious liability where the employer assumes legal responsibility for the actions and behavior of employees,[3] and the like.

Alongside the determination of the purpose of processing, the employer shall assess the proportionality of the information collected, and the ways and means of processing. This principle directs the employer to process information that is adequate, relevant, suitable, necessary and not excessive in relation to the declared and specified purpose.[4]

The methodology of data collection should likewise be proportional to the achievement and fulfillment of the purpose of the employer. Thus, personal data of the employees shall only be collected, used and stored by the employer, through computer monitoring, if the purpose sought to be achieved cannot be fulfilled by any other less privacy intrusive means.

In all cases, the employer is duty-bound to inform and notify the data subjects of the nature, purpose, and extent of computer monitoring and processing when using office-issued computers.[5] Moreover, the employer must issue a policy or set of guidelines on the use of company-issued devices and equipment.

Recommendation

"Secret surveillance" as you mentioned is frowned upon. Regardless of the legitimate purpose of processing, is the duty of the employer to explain the conduct of computer monitoring to the employees, the specific purpose, scope and actual method of monitoring, 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.

The use of a software that records the keystrokes of the user and/or takes random photos of the computer screen seems to be an excessive and disproportionate mechanism in monitoring employees. Unless the declared purpose of computer monitoring necessitates and justifies the use of such extreme measure, the same should not be carried out.

Every employer conducting computer monitoring or employee monitoring should ensure that the data collected directly satisfies the purpose of monitoring and that it clearly aligns with the need and objectives of the organization.[6]

A policy discussing the parameters of monitoring is in order to be able to ensure that the employees still have a reasonable expectation of privacy at work.[7] It is recommended to contain the following information:

- Purpose/s that computer monitoring seeks to fulfill;
- Circumstances of monitoring, including the time and place it may be conducted;
- The kinds of personal data that may be collected in the course of monitoring;

[3] Privacy Commissioner for Personal Data, Hong Kong, Privacy Guidelines: Monitoring and Personal Data Privacy at Work (April 2016), *available at* https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf (last accessed Oct. 26, 2018)
[4] Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (c).
[5] *Id.* § 18 (a).
[6] Privacy Commissioner for Personal Data, Hong Kong, *supra* note 3.
[7] Article 29 Data Protection Working Party, Opinion 2/2017 on Data Processing at Work (08 June 2017), *available at* ec.europa.eu/newsroom/document.cfm?doc_id=45631 (last accessed Sept. 26, 2018).

- Criteria for accessing monitoring records;
- Retention period of recordings or footages;
- Security measures pertaining to the storage, disclosure and disposal of recorded information;
- Authorized personnel who have access and control over the system in place; and
- Procedure on how employees may lodge complaint in case of violation of their rights, including the right to access their own personal data collected.[8]

Employers should keep in mind that although employees are within office premises and using company-issued equipment within office hours, they still are entitled to their right to privacy at work.

In the same way that the companies value the privacy rights of every customer, it should likewise respect the privacy of its own employees and enable them to exercise their rights. With the emergence of new technologies that provide employers with vast opportunities to monitor and track employees, unbridled checking can damage trust, disrupt professional relationships and disturb workplace peace and performance.[9] An effective policy and communication strategy must be implemented to maintain the balance between the business or operational objectives and the right to privacy.

This opinion is based solely on the information you have provided. Additional information may change the context of the inquiry and the appreciation of facts.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

[8] *Supra* note 5.
[9] Privacy Commissioner of New Zealand- Privacy at Work: A guide to the Privacy Act for employers and employees, accessed on 28 November 2018, available at https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-at-Work-2008.pdf