PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2024-003[1]

02 April 2024

[redacted]

Re: RANDOM SURVEILLANCE OF TELECOMMUTING EMPLOYEES AND CONSENT TO THE RECORDING OF VIRTUAL MEETINGS.

Dear [redacted]:

We respond to your request for an Advisory Opinion on the data privacy implications of the employee monitoring policies that your company intends to implement.

You state that your company is a business process outsourcing solutions and information technology-enabled services provider. As such, your employees regularly process personal information of customers, such as their full name, credit card number, card verification number, address, and phone number.

Your company allows its employees to telecommute, or work remotely, using either company-issued equipment or their own device. To provide an additional level of security to prevent mishandling or unnecessary disclosure of confidential data to unauthorized third parties, your company is considering the adoption of certain policies that involve the requisition of web cameras with built-in microphones that will be turned on at random intervals to record short videos (including image and audio) of the subject employee and his/her immediate surroundings. Also, your company intends to record all work-related virtual meetings, conferences, trainings, and coaching sessions.

Thus, you ask whether the Data Privacy Act of 2012[2] (DPA): 1) permits the installation of a monitoring software to randomly record telecommuting employees and their immediate surroundings for purposes of data security; and 2) requires your company to secure the written consent of the employees every time a work-related virtual meetings, conferences, trainings, and coaching sessions (collectively, "virtual meetings") is held.

[1] Tags: Telecommuting, monitoring software, employee surveillance, contract, legitimate interest.
[2] 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).

Reasonable expectation of privacy.

Generally, the factual circumstances of each case determine the reasonableness of the expectation of privacy. Similarly, customs, community norms, and practices may limit or extend an individual's reasonable expectation of privacy. The reasonableness of a person's expectation of privacy is, thus, determined on a case-to-case basis.[3]

Nevertheless, it is worth revisiting our discussion in NPC Advisory Opinion No. 2018-090[4] on the application of this concept in the workplace, *viz*.:

> (C)ourts have generally held that employees have a decreased expectation of privacy with respect to work devices, email accounts, and internet surfing activities. The same may be said for the contents therein, since there is an assumption that its use will be limited to work-related purposes.
>
> Yet, with the DPA now in place, the reasonable expectation test should be revisited and interpreted in the context of the law.
>
> By virtue of a legislation on data protection and privacy, the assumption is that individuals now have an expectation of privacy. As to the second element, data privacy is now more than a reasonable expectation – it is now enshrined in the DPA. The reasonable expectation of privacy test then should take into consideration the standards provided under the DPA.
>
> This means that employees must be aware of the nature, purpose, and extent of the processing of his or her personal data in the workplace. The processing of personal information of employees shall also be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. Lastly, the processing of such information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

Scope of the DPA; personal information; processing; lawful basis; general data privacy principles.

The DPA applies to the processing of personal and sensitive personal information (collectively, personal data) and to any juridical person involved in the processing of personal information.[5] Personal information is defined as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[6]

Processing refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[7]

---

[3] National Privacy Commission, NPC Advisory Opinion No. 2018-090 (28 November 2018).

[4] *Id*.

[5] Data Privacy Act of 2012, § 4.

[6] *Id.* § 3 (g).

[7] *Id.* § 3 (j).

The installation of a monitoring software is considered as processing under the DPA since it involves the collection and/or recording of the employees' personal data. As such, a lawful basis must be established for processing of personal data under either Sections 12 or 13 of the DPA.

In the scenario you provided, your company may rely on either Section 12 (b) or 12 (f) of the DPA. Section 12 (b) of the DPA allows processing for the fulfillment of a contract with the data subject. You may utilize this basis as long as the employment contract provides specific provisions allowing the installation of equipment/software for furtherance of employment, including enhancement of productivity of telecommuting employees to ensure that they adapt with flexible working arrangements, for the protection of the interest of the clients or customers, or the enforcement of company policies. In which case, the installation of monitoring software is justified as a necessary consequence of the employer-employee relationship.

On the other hand, Section 12 (f) of the DPA allows processing if it is necessary for the purposes of the legitimate interests pursued by the PIC. We acknowledge that employers have legitimate business interests, such as management of workplace productivity, service quality control or enforcement of company policies, employee safety, protection of business assets, intellectual property or other propriety rights, prevention of vicarious liability where the company assumes legal responsibility for the actions and behavior of employees, compliance with statutory or regulatory obligations that provide, or give reasonable cause, for the preventive monitoring of employees,[8] amongst others. However, they must ensure that the processing activity should be directly related to the legitimate interest being pursued.

Thus, while the processing of personal information based on the legitimate interests of the PIC is allowed under the DPA, an employer must still assess if the installation of a monitoring software will pass the three-part test of legitimate interest, namely:

1. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;
2. Necessity test - The processing of personal information must be necessary for the purposes of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test - The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PICs or third party, considering the likely impact of the processing on the data subjects.

The processing must also comply with the general data privacy principles of transparency, legitimate purpose, and proportionality. In NPC Advisory Opinion No. 2018-084, we stated that 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. Additionally, the principle of proportionality directs the employer to assess the proportionality of the information collected, and the ways and means of processing. This means that the employer shall process information that is adequate, relevant, suitable, necessary, and not excessive in relation to the

[8] 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 Feb. 23, 2024).

declared and specified purpose. Since the monitoring of the employees' surroundings may result in the capturing of personal data of other individuals, the company should determine whether the data collected is proportional to the achievement and fulfillment of the purpose of monitoring and that it clearly aligns with the need and objectives of the organization.[9] Lastly, to ensure adherence to the principle of transparency, the employer should effectively communicate to the employees, through the issuance and dissemination of a policy, the conduct of employee monitoring, 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.

As to your query on written consent of the employees for virtual meetings, please note that consent may not be the most appropriate basis for such processing since employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the company-employee relationship.[10] Instead, your company may still rely on either Sections 12(b) or 12(f) of the DPA as long as the recording of virtual meetings is work-related. Consequently, you may dispense with the requirement of obtaining the consent of employees every time virtual meetings are recorded.

Privacy Impact Assessment.

Finally, we recommend the conduct of a Privacy Impact Assessment (PIA) prior to the establishment and use of the proposed monitoring software or whenever there is a significant change in the software or software to assess and mitigate risks on the rights and freedoms of data subjects.

A PIA is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or a personal information processor (PIP). It considers the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations.[11]

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

[9] *Id.*
[10] ARTICLE 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, available at https://ec.europa.eu/newsroom/article29/items/610169 (last accessed Feb.22, 2024).
[11] NPC Advisory No. 2017-03, Guidelines on Privacy Impact Assessment, 31 July 2017.