Insight Briefing:

Data Privacy: NPC Addresses Return-to-Work and WFH Questions

7 June 2020

The National Privacy Commission (NPC) has issued a bulletin answering FAQs on returning-to-work and current work-from-home arrangements (*NPC PHE Bulletin No. 14: Updated Frequently Asked Questions (FAQs)*). The full text of the NPC bulletin can be found here: https://www.privacy.gov.ph/2020/06/npc-phe-bulletin-no-14-updated-frequently-asked-questions-faqs/.

The following are some of the key points of the FAQ bulletin.

On returning-to-work

1. **What type/s of personal data can employers collect from employees? Can employers collect health information? How can this be done with the best consideration for privacy?**

   There is a legitimate basis "for employers to collect additional personal data that includes health information from employees during the pandemic." Employers "may collect personal data that are necessary for a specified and legitimate purpose to help control the spread of the virus and keep their workers and visitors safe."

   In collecting and processing data, including health data, from employees, "employers are enjoined to adhere to data privacy principles of transparency, legitimate purpose and proportionality. Keep collection to the minimum information necessary and use appropriate means to achieve the purpose. It is essential for employers to be transparent with their employees during this time."

   Once collected, "reasonable and appropriate safeguards should be in place to ensure the security of the physical or electronic forms used" (*i.e.,* health symptoms questionnaires or health status survey forms under the custody of the employer).

   Employers should "set a health information policy within the company considering the following, among others: determination of who is authorized to gather the information, who should know the results, how to secure the information, and how to disclose it to authorities when necessary."

2. **How long can employers retain the personal data that they have collected?**

   Employers may retain the personal data of employees to the extent necessary "to fulfill the purpose for which these were collected, pursuant to the protocols of the relevant public authorities." After the fulfillment of such purpose/s, "personal data shall be disposed in a secure manner that would prevent any unauthorized processing."

3. **In keeping with implementing the minimum health standards, can employers regularly check the temperature of employees returning to work? Can employees refuse to have such temperature checks?**

   Yes. Employers "may regularly check the temperature of employees returning to work."

   According to Department of Health (DOH) *Department Memorandum No. 2020-0220*, "employees physically reporting to their workplaces shall be screened for COVID-19 symptoms, including fever, cough, colds, and other respiratory symptoms. Daily temperature and symptom monitoring and recording of all staff who will report for work are part of prevention and control measures."

   Hence, "it is necessary to conduct temperature checks under existing issuances of various public authorities. Employees should find it reasonable to be screened and must cooperate with their employers to ensure the safety of all returning employees. Employers are expected to use reasonable measures to ensure privacy when doing the collection, like instructing security guards or other personnel to refrain from publicly announcing a person's temperature results and putting in place protocols to implement minimum health standards mindful of the rights and freedoms of data subjects."

4. **Can employers continue checking for travel history and data?**

   Yes. Travel history can still be included in usual medical assessments. "Employers may collect such data in compliance with the DOH requirements."

5. **Can employers disclose to other parties the health information collected from employees? Can it be used for other purposes? Can they reveal these data to health authorities?**

   Any disclosure of employee health data related to COVID-19 must be limited to the (a) DOH, (b) "entities authorized by the DOH," and (c) "entities authorized by law," and must be in accordance with all existing protocols on the matter. "Use of collected employee data shall solely be for the specified and declared purpose/s only."

6. **Can employers retain information collected about employees' temperature checks, results of antibody testing, and/or COVID-19 diagnosis? How long can they retain such information?**

   Yes. "Temperature checks, results of antibody testing, and/or COVID-19 diagnosis may be retained as necessary to fulfill the purpose for which these were collected, pursuant to the protocols of the relevant public authorities.

Retention requires that appropriate security measures (*i.e.* organizational, physical, and technical) are implemented in order to prevent unlawful processing or unauthorized access by other employees or third parties."

On Work-from-home (WFH)

7. Can employers monitor employees during WFH through the installation of monitoring software in company-issued devices?

Yes. Employers, in exercising their legitimate interest, "may monitor employees during WFH but should balance it with the rights and freedoms of their employees and adherence to the general data privacy principles." According to *NPC Advisory Opinion No. 2018-048*, "monitoring employee activities when he or she is using an office-issued computer may be allowed" under the Data Privacy Act, provided that "the processing falls under any of the criteria for lawful processing" under the law.

Employers "must be transparent to the employees and notify them that they are being monitored." There should be "an assessment of the necessity and proportionality of the monitoring" (*i.e.,* the method of monitoring) vis-à-vis "the objective of the same" (*i.e.,* ensuring productivity during WFH). "It is also recommended for the employers to conduct a privacy impact assessment of the monitoring software to determine risks and how to mitigate them. Employers should likewise implement clear policies with regard to its monitoring procedures."

Further, "less privacy-intrusive means of monitoring should be considered rather than excessive and disproportionate mechanisms" in monitoring such as "the use of tracking mouse movements, recording keystrokes, taking random photos of the computer screen, enabling webcams to take a picture of the employee, etc."

8. Can employers require employees to stay on video during business hours or even beyond as when they render overtime work, as proof of work done during the day?

No. The proportionality principle dictates that "the processing of information shall be adequate, relevant, suitable, necessary, and not excessive." Personal data "shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means." Employers "should avoid extreme privacy-intrusive means of managing employees as there are other available means of ensuring that employees are doing their assigned tasks."

9. How can employers ensure that personal data processing systems being used during WFH are secured?

Employers "can secure personal data processing systems being used during WFH" by providing proper information and communications technology equipment and "support facilities and mechanisms to the employees." More importantly, "data protection and privacy policies should be in place to guide the staff."

> Specifically, for the government, "the heads of agencies shall ensure that employees have access to or is provided with communication equipment or facilities (laptop, computer, internet, telephone, mobile phone, etc.) to carry out their functions."

For more information about the legal issuances discussed in this briefing, please contact –

Rose Marie M. King-Dominguez
Partner
rmmking@syciplaw.com

SyCip Salazar Hernandez & Gatmaitan
SyCipLaw Center, 105 Paseo de Roxas
Makati City 1226, The Philippines
t: +632 8982 3500; +632 8982 3600; +632 8982 3700
f: +632 8817 3145; +632 8817 3896
e: sshg@syciplaw.com
www.syciplaw.com