Data Privacy and WFH: NPC Bulletin on Protecting Personal Data in a Work From Home Arrangement

The National Privacy Commission (NPC) has issued guidelines on data protection in work from home (WFH) arrangements (NPC PHE Bulletin No. 12 on "Protecting Personal Data in a Work from Home Arrangement; issued May 15, 2020). The full text of the guidelines can be found here: https://www.privacy.gov.ph/2020/05/npc-phe-bulletin-no-12-protecting-personal-data-in-a-work-from-home-arrangement/.

The following are some of the key points of the NPC's WFH guidelines:

1. **Authorized Information Communication Technology (ICT) Assets.** Organizations are responsible for making sure telecommuting employees are provided the proper ICT assets. In return, the employees are accountable and responsible for the physical care of those assets.

    a. *Computer and other ICT peripherals.* Employers should issue their staff with appropriate ICT resources to adequately perform their duties. Personal devices may be used if provision of organization-owned ICT resources is impractical. Such practice, however, must be governed by the organization's Bring Your Own Devices (BYOD) policy.

    b. *Removable Devices.* Personnel are encouraged to only use organization-issued ICT peripherals (such as USB flash drives, USB mouse, USB keyboard, etc.). When using portable media (such as disks or USB flash drives) to store or transfer data, the use of data encryption must be ensured.

    c. *Software.* Only software authorized by the organization must be used and only for official purposes. Avoid storing the organization's digital files, including those with personal data, on external services and software.

    d. *Proper configuration and security updates.* Install security patches prior to and while WFH is enforced to prevent cyber security exploits and malicious damage.

    e. *Web Browser Hardening.* Ensure that your browser is up to date and properly configured. The NPC bulletin lists the configurations for popular browsers such as Chrome, Firefox, and Edge.

    f. *Video conferencing.* If available, only use video conferencing platforms contracted by your organization, which should pass its privacy and security standards. When availing

of free platforms, use only an up-to-date version, one that offers adequate privacy and security features, and is properly configured.

2. **Acceptable Use.** Organizations must have an Acceptable Use Policy ("AUP") that defines allowable personal uses of ICT assets. While organization ICT assets should only be used for authorized purposes, the AUP must acknowledge that occasional personal use by employees may occur without adverse effect to the organization's interests. The AUP should also define unacceptable and unauthorized uses.

3. **Access Control.** Personnel access to organization data must only be on a "need-to-know basis," anchored on pre-defined user profiles and controlled via a systems management tool.

4. **UserAuthentication.** Require strong passwords to access personnel credentials and accounts. Passwords must be at least eight (8) characters long, comprising upper- and lower-case letters, numbers and symbols. Prohibit sharing of passwords. Set up multifactor authentication for all accounts to deny threat actors immediate control of an account with a compromised password.

5. **Network Security.** When organization ICT assets are connected to personal hotspots and/or home Wi-Fis, observe the security measures listed in the NPC bulletin, such as avoiding malicious webpages, ensuring high availability and reliability of internet connection, configuring the Wi-Fi Modem or Router, and avoiding connecting office computers to public networks.

6. **Records and File Security.** Set up policies to ensure sensitive data is processed in a protected and confidential manner to prevent unauthorized access.

7. **Emails.** When transferring sensitive data via email, encryption of files and attachments should be done. Also, ensure that personnel always use the proper "TO, CC, and BCC" fields to avoid sending to wrong recipients or needlessly expose other people's email addresses to all recipients.

8. **Physical security.** Create workspaces in private areas of the home, or angle work computers in a way that minimizes unauthorized or accidental viewing by others. Lock away work devices and physical files in secure storage when not in use. Should there be a need to print documents, the personnel must ensure that physical and digital documents are properly handled and disposed of in accordance with office policy. Never leave physical documents with sensitive data just lying around, nor use them as "scratch paper."

9. **Security Incident Management.** Personnel must immediately notify his or her immediate supervisor in case of a potential or actual personal data breach while working from home. The organization's Data Protection Officer and/or Data Breach Response Team should immediately be alerted.

This bulletin was prepared by the SyCipLaw TMT Group.

For more information about the legal issuances discussed in this bulletin, please contact:

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

This bulletin contains a summary of the legal issuances discussed above. It was prepared by SyCip Salazar Hernandez & Gatmaitan (SyCipLaw) to update its clients about recent legal developments.

This bulletin is only a guide material and is circulated for information purposes only. SyCipLaw assumes no responsibility for the accuracy, completeness or timeliness of any information provided in this bulletin. It does not constitute legal advice of SyCipLaw or establish any attorney-client relationship between SyCipLaw and the reader. It is not a substitute for legal counsel. Online readers should not act upon the information in this bulletin without seeking professional counsel. For more specific, comprehensive and up-to-date information, or for help regarding particular factual situations, please seek the opinion of legal counsel licensed in your jurisdiction.

SyCipLaw may periodically add, change, improve or update the information in this bulletin without notice.

Please check the official version of the issuances discussed in this bulletin. There may be other relevant legal issuances not mentioned in this bulletin, or there may be amendments or supplements to the legal issuances discussed here which are published after the circulation of this bulletin.

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