FREQUENTLY ASKED QUESTIONS (FAQs) ON NPC CIRCULAR NO. 2023-06

SECURITY OF PERSONAL DATA IN THE GOVERNMENT AND THE PRIVATE SECTOR

GENERAL PROVISION

I. WHAT IS THE DIFFERENCE BETWEEN CIRCULAR NO. 2023-06 (SECURITY OF PERSONAL DATA IN THE GOVERNMENT AND PRIVATE SECTOR) AND CIRCULAR NO. 2016-01 (SECURITY OF PERSONAL DATA IN GOVERNMENT AGENCIES)?

Circular No. 2016-01 pertains to the security of personal data in government agencies and is limited to government agencies engaged in the processing of personal data. On the other hand, Circular No. 2023-06 applies to all natural or juridical persons engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the DPA, its IRR, and other relevant issuances of the NPC. Thus, it covers both the government and the private sectors.

Circular 2023-06 repeals Circular 16-01, removing outdated sections and adding new sections such as privacy-by-design, privacy-by-default, and business continuity. General requirements were added to provide organizations with more flexibility in identifying the appropriate security measures.

II. ARE PERSONAL INFORMATION CONTROLLERS (PICs) NOW REQUIRED TO TRAIN ALL THEIR PERSONAL INFORMATION PROCESSORS (PIPs) ON PRIVACY AND DATA PROTECTION?

Under Section 4(f) of Circular 2023-06, training its personnel is part of PICs' and PIPs' responsibility. It does not, however, require a PIC to train its PIP. However, PICs should ensure that the PIPs they engage with have implemented adequate protection and training on privacy and data protection policies.

III. WILL THE NPC ORDER THE PIC TO SUBMIT THE PIP'S PRIVACY AND DATA PROTECTION POLICIES?

Following on-site visits, compliance checks, and data breach notifications, the NPC may require the submission of the PIC's data protection policies, policies pertaining to third parties, and contracts for review. However, submission of PIP's policies is not required.

STORAGE OF PERSONAL DATA

IV. IS THERE A DEFINITION FOR HIGH VOLUME OF DATA?

There is no current definition of high volume of data. However, the criteria for registration to the NPC, as stated in Section 5 of NPC Circular 2022-04, may serve as the baseline for a high volume of data.

ACCESS TO PERSONAL DATA

V. DOES ACCESS MEAN ONLY PHYSICAL ACCESS?

No, access can be physical or online. Rule IV of the Circular covers security measures for online and physical access to personal data. Online access may cover access to information systems, databases, documents stored in the cloud, etc. Physical access occurs when personal data is stored in any physical media, such as a paper-based filing system.

VI. WILL THE PRESENCE OF A USERNAME, PASSWORD, AND APPROVER WHEN ACCESSING PERSONAL DATA WITHIN THE ORGANIZATION'S NETWORK SUFFICE TO MEET THE REQUIREMENT OF SECURITY MEASURES?

Merely having a username, password, and approver may not be sufficient to meet the full requirements for accessing within an organization's network. Rule IV of the Circular provides the requirements for security measures related to access to personal data. In addition, a PIC or a PIP is in the best position to determine appropriate security measures to implement since it has knowledge of its IT infrastructure.

TRANSFER OF PERSONAL DATA

VII. IS THE USE OF A FAX MACHINE ALLOWED IF THE OFFICE LOCATION HAS NO ACCESS TO THE INTERNET AND THE ONLY WAY TO TRANSMIT PERSONAL DATA IS VIA FAX MACHINE?

No, fax machines pose a high privacy risk; hence, Section 26 of the Circular explicitly prohibits the use of fax machines or facsimile technology. In this day and age, technologies offer alternatives that provide data encryption for transmitting documents containing personal data that are accessible through several platforms.

Section 27 of the Circular discusses other means of transmitting documents. It states that a PIC and its PIP that transmits documents or media containing personal data by mail or post shall use registered mail or, where appropriate, guaranteed parcel post services and Private Express and/or Messengerial Delivery Service (PEMEDES).

MISCELLANEOUS PROVISIONS

VIII. WHAT CAN TRIGGER AN AUDIT OF THE PICS' OR PIPS' COMPLIANCE WITH THE DPA OF 2012?

An audit can be triggered by various factors, such as investigations due to complaints, reported breaches involving personal data, or part of regular monitoring and enforcement activities of the NPC, such as compliance checks.

IX. DOES THE NPC HAVE ACCREDITED INDEPENDENT PARTIES, OR IS THE ORGANIZATION ALLOWED TO ENGAGE ANY INDEPENDENT PARTIES TO CONDUCT VERIFICATION?

The NPC does not accredit or specifically endorse any independent or third-party organizations for verifying or auditing PICs or PIPs. The Circular does not prohibit PICs or PIPs from engaging with independent parties to conduct audits, but it does not require them to engage in independent verification or certification by a third party.

X. WHEN WAS THE CIRCULAR PUBLISHED IN A NEWSPAPER OF GENERAL CIRCULATION?

The Circular was published in the Daily Tribune on March 15, 2024.

XI. WHEN IS THE EFFECTIVITY OF THIS CIRCULAR?

The Circular took effect on March 30, 2024. As provided in Section 40 thereof, the Circular takes effect fifteen (15) calendar days from the time it was published in a newspaper of general circulation.