

Asia Internet Coalition Comments on the Philippines NPC Repeal of Circular 16-01 ([Draft NPC Circular](#)): Security of Personal Data in the Government and the Private Sectors (2nd Public Consultation)

21 April 2023

Atty. John Henry Du Naga
Commissioner and Chairman
National Privacy Commission (NPC)

Subject: Asia Internet Coalition Comments on the Philippines NPC Repeal of Circular 16-01 ([Draft NPC Circular](#)): Security of Personal Data in the Government and the Private Sectors (2nd Public Consultation)

On behalf of the Asia Internet Coalition (AIC) and its members, I am writing to express our sincere gratitude to the National Privacy Commission (NPC), for the opportunity to submit comments on the **2nd Public Consultation regarding Circular 16-01 ([Draft NPC Circular](#)) regarding Security of Personal Data in the Government and the Private Sector**. AIC is an industry association comprised of leading internet and technology companies in the Asia Pacific region with a mission to promote the understanding and resolution of Internet and ICT policy issues in the Asia region.

We acknowledge the importance of this consultation that outlines the key elements of data privacy, with an objective of having a safe and secure online environment, and align with global best practices. In the past, AIC has been very active in submitting industry recommendations on some of the key policy issues in Asia, [details of which can be accessed here](#).

In the backdrop of digitalization and growth of digital services across the world, the role of data has become more and more significant. This has given rise to concerns of informational privacy and the exercise of rights over personal data. Without a framework to govern these two subjects, no digital industry can be sustainable.

In this regard, we are grateful to be able to present our **comments and recommendations in Appendix A** of this paper and would also like to re-state our continuous support and assistance to the Philippines government in its efforts to bring about this transformational change in the privacy landscape. As such, please find appended to this letter detailed comments and recommendations, which we would like to respectfully request the National Privacy Commission to consider.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration. Importantly, we would also be happy to offer our inputs and insights on industry best practices directly through meetings and discussions to help shape the dialogue for an effective privacy regime in the Philippines.

Sincerely,



Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Appendix A

Section #	Requirements	Recommendation
SECTION 6	Privacy Impact Assessment. - A PIC shall ensure that its conduct of a Privacy Impact Assessment is proportionate and consistent with the amount and sensitivity of the personal data being processed, and the adverse risks which may arise from the unauthorized processing of personal data. The Privacy Impact Assessment shall include the following A. the types of personal data held by the PIC, including records of its own employees;	Need clarity on “records of its own employees”. Is NPC referring to the list of employees who may have access to the data (which should be managed and maintained via a separate access policy & process) , or is NPC stating that processing records of all employees’ data need to be tracked in data inventory maps?
SECTION 9	The data subject has the right to be informed especially when automated processing becomes the sole basis for making decisions about them and when such decisions would significantly affect them. The software application shall be documented, and the PIC shall notify the Commission and data subjects upon registration of the data processing system with the Commission, and on such other instances as may be required by the Commission. Such notification shall follow the requirements in Section 8 of this Circular and provide the following information: i. Methods and logic utilized for automated processing;	We respectfully request that Section 9 be removed. Section 9 imposes disclosure requirements that are excessively burdensome to companies without a substantially equivalent value-add to consumers. • Excessive Scope - Section 9 requires notification of any wholly or partly automated operation used to make (any) decisions regarding a data subject, regardless of severity of impact/risk. Considering that digital service providers employ some degree of automated processing in essentially all their operations, the amount of effort and resources required to notify NPC on all of these systems is excessively burdensome, without any clear value addition. • Risk to business, cybersecurity - The revised draft obligates organizations

Section #	Requirements	Recommendation
	and ii. Decisions relating to the data subjects that would be made based on processed data or that would significantly affect the rights and freedoms of the data subjects.	to notify NPC of information that may include proprietary and competitively sensitive info (e.g.: Methods and logic utilized for automated processing). Companies face the risk of excessive disclosure requirements which could harm competitiveness and even negatively impact the effectiveness of AML and anti-fraud activities. At a minimum, we request that Section 9.(A)(7) [Methods and logic utilized for automated processing] be removed to avoid disclosure of commercially sensitive information and to maintain cybersecurity. • Misalignment with global privacy laws - Even relatively prescriptive privacy laws such as China's PIPL and EU GDPR don't require such detailed notification for automated systems. Any information to be provided to the public is already captured under the transparency principle of the Data Protection Act's implementation regulations. Request that the additional notification requirements in Section 9 be removed as they create excessive compliance burden for companies. The reason to remove section 9 is that there could be proprietary concerns and trade secrets as part of an automated processing or AI setup. Exposing the methods and logic of AI systems may result in misuse and abuse (especially those used to detect and combat fraudulent activities) and concerns of confidentiality or disclosure of proprietary information/trade secrets. We also seek clarity on what sort of activities constitute "significantly affect" - in the case of the GDPR, there is some context around this insofar as it is preceded by "<u>legal effects...or</u> significantly affects him or her"
SECTION	General Rule. - Personal data being processed by a PIC	PIC may not be in the best position to demonstrate to the Commission how an

Section #	Requirements	Recommendation
10.	shall be stored in a data center, which may or may not be owned and controlled by such PIC: Provided, that the PIC must be able to demonstrate to the Commission how its control framework for data protection, and, where applicable, that of its service provider, shall ensure compliance with the Act: Provided further, that where a service provider is engaged, the Commission may require the PIC to submit its contract with its service provider.	external party (e.g. vendor) operates its control framework. PIPs who are in the business of making profit based on offering data center services (e.g. a tech behemoth offering cloud services to a small-medium enterprise) should be the primary party to demonstrate their control frameworks. Contractual arrangements should be kept confidential and should not be revealed to external parties, unless there is a compelling reason to do so. Commission should put forth the conditions on when such documents ought to be produced (e.g. data breach investigations)
SECTION 11.	Encryption of Personal Data. - All personal data that are digitally processed must be adequately protected, whether at rest or in transit	Suggest to rephrase header, as “encryption” is not the only control mechanism to protect data.
SECTION 13.	Service Provider as Personal Information Processor. - When a PIC engages a service provider for the purpose of storing personal data under the PIC’s control or custody, the service provider acts as a PIP. It is the responsibility of the PIC to ensure that its PIP has implemented appropriate security measures for the protection of personal data and is able to demonstrate compliance with all the requirements of the DPA, its IRR, and all applicable issuances by the Commission. The obligation to comply with all the requirements of the DPA, its IRR, and all applicable issuances by the Commission with regard to the particular data processing system shall remain with the PIC.	PIP is subjected to contractual obligations. PIC may not be in the position to demonstrate that PIP complies with all the requirements of the DPA, its IRR, and all applicable issuances by the Commission. Further, PIPs in the business of making profit based on offering data storage services (e.g. data centre services) may be much better placed to demonstrate how it has implemented appropriate security measures as opposed to a small PIC who is reliant entirely on the expertise of such PIP (e.g. small-medium enterprise), such lack of expertise being the first reason it chose to outsource such service to a service provider in the first place. However, PIC can ensure that PIP warrants that all obligations in the DPA can be complied with, and should the situation arise, for PIP to demonstrate its compliance of the DPA, IRR and applicable issuances to the Commission.
SECTION	Audit. - The Commission reserves the right to audit a	When read with Section 13 and 18, does this mean that PICs are expected to stipulate

Section #	Requirements	Recommendation
14	PIC's data center, or, where applicable, that of its service provider.	in the contracts with PIPs that all PIPS (including foreign PIPs) have to agree to NPC's right of audit (which currently has no clear scope and boundaries)? Will NPC otherwise have the regulatory right to request an audit, regardless of whether this right is agreed to in a contract or not? We would also like to seek clarification that the provision in Section 14 will have no extraterritorial application.
SECTION 17	Security Clearance. - A PIC shall strictly regulate access to personal data under its control or custody. It shall grant access to personnel, through the issuance of a security clearance by the PIC/PIP head, only when the performance of official functions or the provision of a public service directly depends on such access or cannot otherwise be performed without such access. A copy of each security clearance must be filed with the PIC's Data Protection Officer.	To what extent can the role of access provisioning be delegated downstream? How detailed must a request (and consequent clearance) be? This can be operationally cumbersome in the case of large organisations with many employees (does this mean the PIC/PIP head must authorize each individual employee before access is granted)? Examples could be provided by NPC so that organisations know what the required standard is.
SECTION 20	A PIC or PIP shall adopt and utilize technologies that prevent personal data accessible online to authorized personnel from being copied to a local machine or the computer that a user is currently using on a computer network. A PIC or PIP shall also provide technologies for the automatic deletion of temporary files that may be stored on a local machine by its operating system. Where possible, a PIC or PIP personnel shall not be allowed to save files to a local machine. The personnel shall be directed to only save files to their allocated network drive.	We respectfully request that Section 20 be removed. Section 20 imposes requirements that are impossible to comply with in certain scenarios, and generally unclear. • Practicality - There are often scenarios, such as network drives going down or being hacked, where saving and working off local copies of databases that contain personal data may be necessary. Suggest removal of this requirement as security concerns can largely be addressed through appropriate access controls covered in Section 19. • At a minimum, we strongly suggest that NPC lay down its interpretation of

Section #	Requirements	Recommendation
	Drives and USB ports on local machines shall also be disabled as a security measure. A PIC or PIP shall also consider prohibiting the use of cameras in areas where sensitive personal information is visible or processed. Generally, local copies of personal data shall not be accessed, processed or stored on local machines without appropriate security control measures and protection that prevents unauthorized access. A PIC or PIP shall ensure that its personnel are capable and equipped with effective end-to-end protection tools when accessing, using, or storing personal data.	"where possible" and "generally", and describe exceptional situations where local copies can be used (similar to the scenarios described in the previous bullet).
SECTION 21	Local Copies of Personal Data Accessed Online. - A PIC shall adopt and utilize technologies that prevent personal data accessible online to authorized personnel from being copied to a local machine or the computer that a user is currently using on a computer network. The PIC shall also provide for the automatic deletion of temporary files that may be stored on a local machine by its operating system. Where possible, PIC personnel shall not be allowed to save files to a local machine. They shall be directed to only save files to their allocated network drive. Drives and USB ports on local machines may also be disabled as a security measure. A PIC may also consider prohibiting the use of cameras in areas where personal data is displayed or processed.	It does not seem realistic to expect all organisations to adopt technologies that will prevent their employees from downloading files containing personal data to their local workstations. This is likely to impede the operations of organisations and/or be extremely costly for organisations to implement, especially for smaller organisations. Perhaps NPC can look into the availability and practicality of existing solutions, and into certain criteria to be met before this obligation kicks in.
SECTION	Remote Disconnection or Deletion. - A PIC shall adopt	NPC to provide more details on the construct of the proposed notification system.

Section #	Requirements	Recommendation
23.	and use technologies that allow the remote disconnection of a mobile device owned by the PIC, or the deletion of personal data contained therein, in the event such mobile device is lost. A notification system for such loss must also be established.	To clarify if “mobile device owned by the PIC” should be construed strictly, or if it is intended to include authorized devices (as mentioned in Section 22) which may or may not be owned by the PIC.
SECTION 24.	Physical Filing System. - If personal data is stored in any physical media, such as paper-based filing system, a PIC shall maintain a log, from which it can be ascertained which file was accessed, including when, where, and by whom. Such log shall also indicate whether copies of the file were made. The PIC management shall regularly review the log records, including all applicable procedures	Will be useful to have actual scenarios provided. At face value, it seems to be unrealistic and excessively inconvenient for organisations. If I have a file containing lost-and-found forms, does it mean each time an employee flips the file, someone (it can be that employee himself/herself) has to record that activity in a log. And if this log is a physical log, each time an employee looks at the log, a second separate log will have to be maintained?
SECTION 26.	Telecommuting. - The Commission supports the adoption of a telecommuting or alternative work arrangements as a viable strategy to balance the health and safety of a PIC’s or PIP’s workforce with its need to continuously operate and provide essential products and services. A PIC shall define, implement, and communicate its telecommuting policy to its personnel to equip and prepare them	As clarified during the call on 21st December, telecommute arrangements may stem also from a cost benefit, staff morale perspective. Suggest NPC to reword this.
SECTION 27.	Business Continuity Management. - A PIC must have a Business Continuity Plan to mitigate potential operational disruptions due to unforeseen events. It must consider the following: i. Personal data backup, restoration and remedial time; ii. Periodic review and testing of the business continuity	Suggest removal of this Section. BCM should be a part of corporate governance, and the requirements need not be captured in the circular or managed as part of privacy

Section #	Requirements	Recommendation
	plan which takes into account disaster recovery, privacy/business impact analysis, and crisis communications plan, among others; and iii. Contact information and other business-critical matters, i.e., electrical supply, building facilities, IT assets, etc.	regulations.
SECTION 29	A PIC shall implement access controls to prevent themselves and its PIP's personnel from printing or copying personal data to personal productivity software like word processors and spreadsheets that do not have any security or access controls in place	More guidance may be necessary on what NPC deems to be adequate security/access controls for personal productivity software.