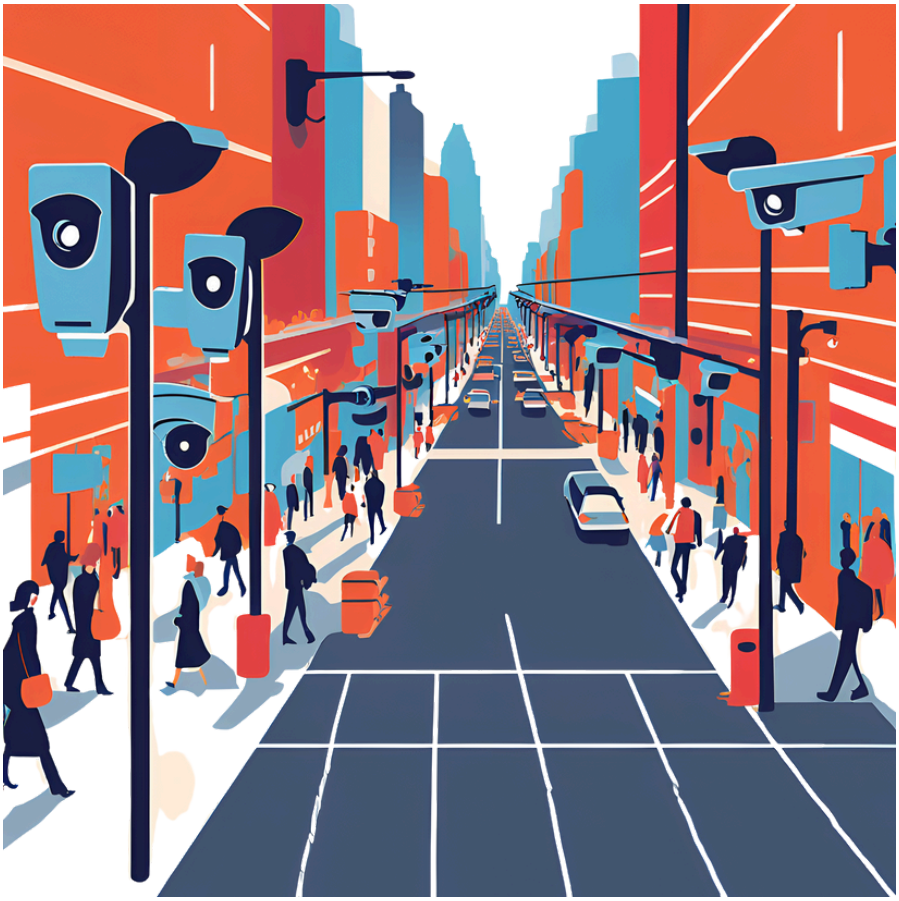
CCTV Systems and Data Protection

PRIVACY.PH
COLLECTIVE



CCTV Systems and Data Protection

PRIVACY.PH
COLLECTIVE

https://www.facebook.com/groups/privacy.ph

Quezon City
PRIVACY.PH Collective
2024

The **PRIVACY.PH COLLECTIVE** is a community of individuals dedicated to promoting privacy and data protection in the Philippines. Through regular meetups, the collective aims to create a safe and engaging space for discussions on both current and emerging issues. It also focuses on developing accessible reference materials and guidance documents, catering to specific sectors, industries, and the general public. The group aspires to cultivate privacy advocates who actively address privacy and data protection concerns across various platforms. Additionally, it aims to build a credible pool of resource persons available for trainings, workshops, and other speaking engagements.

This primer is the first of many materials the group plans to develop. Succeeding versions may include additional content, as well as revisions or modifications of current content.

Questions and suggestions may be relayed via *info@privacyphl.com* or the Facebook group: *PRIVACY.PH*.

Contributors

Chen Argote
Karl Baquiran
Danny Cheng
Shari Datu Tambuyung
Rej Estillore-Gonda
Jam Jacob
Mike Laxina
Maris Miranda
Jess Pacis
Jen Paguntalan-Balane

Layout and Design

Jam Jacob

Photo and Artwork

AI-generated

Acronyms

CCTV	Closed-Circuit Television
DILG	Department of the Interior and Local Government
DPA	Data Privacy Act of 2012
IRR	Implementing Rules and Regulations
NPC	National Privacy Commission
PIA	Privacy Impact Assessment
PIC	Personal Information Controller
PIP	Personal Information Processor
SPI	Sensitive Personal Information

GENERAL INFORMATION

Is CCTV footage considered personal information or sensitive personal information?

The NPC suggests that it can be both, when it says that CCTV systems process both personal information and sensitive personal information.[1] However, the agency stops short of offering concrete, useful examples.

On the other hand, in an old Advisory Opinion, the NPC explained that CCTV footage or image could reveal sensitive personal information, implying that a CCTV footage/image on its own is not an SPI.[2] It's what it can reveal or disclose that may be classified as SPI.

Can you give scenarios where CCTV footage is considered sensitive personal information?

The NPC has previously advised that images could themselves be considered as SPI if they feature or reveal information that are clearly defined as such. In the past, it has classified the following as SPI:

- photographs connected to a crime allegedly committed by the data subjects[3]
- images that do not only identify students, but also reveal other education-related details, like the name of their school, grade level, exam scores, etc.[4]

It may be argued that this also applies to CCTV footage. For instance, if CCTV footage records the presence of a data subject in a political event or catches him spending time with a particular politician, one might argue that the CCTV footage establishes his political affiliation. Similarly, when a CCTV footage shows a person in a particular place of worship or healthcare institution, it might suggest his religion or medical condition. As per the DPA, political and religious affiliation, as well as health information, are all classified as SPI.[5]

Are dash cams covered by NPC Circular 2024-02?

That appears to be the case—at least to the extent that they are not used purely for personal, family, or household purposes.

This may be inferred from the Circular which says it covers CCTV Systems that monitor public spaces,[6] and then goes on to define public spaces as including:

- public utility vehicles, and
- private vehicles covered by app-based transport network services (also known as transport network vehicle services or "TNVS") [7]

When is the use of CCTV systems by homeowners covered by NPC Circular 2024-02?

Ordinarily, the Circular does not apply to the use of CCTV systems for purely personal, family, or household affairs.[8] This means their use is not connected to any professional activity and is not intended for profit or commercial gain.[9] A good example would be when it is used by homeowners to secure the premises and boundaries of their private and non-commercial residence or establishment.[10]

However, when CCTV systems capture the images of individuals beyond the boundaries of said residence or establishment, its use can no longer be considered as purely for personal, family, or household purposes—says the NPC.[11] Accordingly, such use will be covered by the Circular and data protection regulations, in general. A good example would be when a CCTV system monitors public space[12] (e.g., streets and alleys, sidewalks, public parks, malls, public utility vehicles, etc.).[13]

How does NPC Circular 2024-02 impact homeowners who rent out their properties, (e.g., as Airbnb hosts)?

Homeowners who operate a CCTV system while renting out their property are covered by the Circular. This is because their use of said System is already connected to a professional activity or one that is intended for profit or commercial gain.

In the case of Airbnb hosts, however, it is important to note that beginning 30 April 2024, they are already prohibited from operating indoor security cameras, while their use of exterior security cameras is now subject to stricter rules.[14]

How should a homeowner position his CCTV camera in order to reduce the risk of non-compliance?

A homeowner should avoid placing his CCTV camera in locations where it can capture footage outside the boundaries of his property, such as public spaces.[15] Areas with heightened expectation of privacy should also be avoided.

Did NPC Circular 2024-02 repeal NPC Advisory 2020-04?

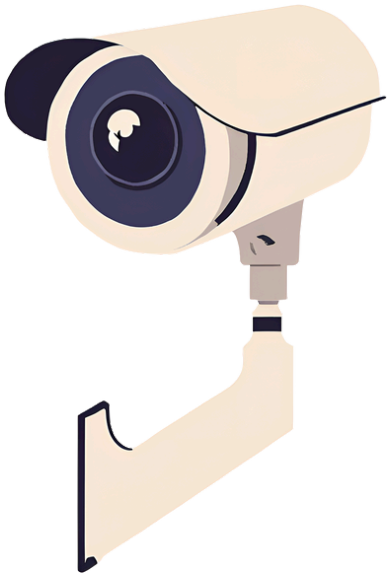
NPC Circular 2024 (Closed-Circuit Television Systems) has *not* explicitly repealed NPC Advisory 2020-04 (Guidelines on the use of Closed-Circuit Television Systems). Instead, it simply states that all other rules, regulations, and issuances that are contrary to or inconsistent with its provisions are deemed repealed or modified.[16]

In theory then, any additional directives or instructions featured in the Advisory that do not contradict or undermine the Circular remain valid. Because they are found in an Advisory, though, they function more as guidelines or recommendations.

What will happen if the use of a CCTV system violates NPC Circular 2024-02?

When the use of a CCTV system violates the Circular, it carries with it potential criminal, civil, and administrative liabilities.[17]

For instance, the erring party may be charged with the crime of unauthorized processing of personal information. It may also be fined by the NPC if its violation qualifies as an infraction of any of the general privacy principles or data subject rights enshrined in the DPA.[18] A data subject who suffers harm because of the improper or unauthorized use of a CCTV system could also file an action for damages against its owner/user.[19]



INSTALLATION

How does one justify the deployment and use of a CCTV system?

A PIC can justify its use of a CCTV system by identifying an appropriate legal basis. To accomplish this, it must refer to the criteria listed in Sections 12 and 13 of the DPA.[20] For example:

- **Consent**. While it is theoretically possible to use consent as a legal basis, it is not the most suitable or practical given the context within which CCTV systems operate.[21] It would be extremely difficult, if not impossible, to ask for the permission of every individual whose image might be captured by one's CCTV camera, especially when it covers public or semi-public places.

- **Legal obligation**. An establishment can install and operate a CCTV system if it is required by law or a regulation to do so. This is true especially for those covered by local government ordinances that make it mandatory to operate CCTV systems.

- **Legitimate interests**. To the extent that they do not collect and process sensitive personal information, CCTV System use can be justified by the owner's pursuit of its legitimate interests (e.g., keeping its property secure).

What are some points to consider when installing or deploying a CCTV system?

When deciding how to install or deploy a CCTV system, some details worth considering include:

1. purpose of the monitoring [22]
2. location and angles of the cameras [23]
3. system capabilities (e.g., zoom, rotation, audio-capture, storage, etc.) [24]
4. nature of covered spaces (e.g., public space, semi-public space, space with heightened expectation of privacy, etc.) [25]
5. quality of the recorded data [26]

What is considered an appropriate and suitable quality for a CCTV footage?

The NPC has not offered guidance in terms of what it considers to be CCTV footage that is of appropriate and suitable quality. However, other government agencies and local government units have.

The Department of the Interior and Local Government (DILG), for instance, has recommended minimum specifications for CCTV systems it is requiring local government units to put up.[27] They include:

- High-definition analog or at least 2 Megapixel Digital Camera
- 0.1 Lux Minimum Illumination
- 30 frames-per-second recording capability per camera
- Analog High-Definition Input (1080p@25FPS, 1080@30FPS, 720@25FPS, 720@30FPS)

One may refer to the actual issuance for the complete set of recommendations.

Is a PIA required before deploying a CCTV system?

The NPC does not explicitly indicate that a PIA must be conducted first before a CCTV system is deployed.

However, it does say that a PIA should be undertaken for every data processing system of a PIC or PIP.[28] So one could argue that even if a PIA need not necessarily be undertaken prior to the deployment of a CCTV system, it is certainly expected at some point, while the system is in use.

At the same time, the NPC also states that when establishing policies on the operation of CCTV systems, a PIC should include the regular conduct of PIAs.[29] And then, when one uses video analytics (e.g., to detect a person or vehicle entering a restricted area) to process personal data derived from CCTV systems, the agency also requires a PIC to carry out a PIA to assess and minimize potential privacy risks.[30]

What information should be included in a CCTV Notice?

Since a CCTV notice is a specific kind of privacy notice, all information one expects to see in the latter must also be featured in a CCTV notice.[31] As a minimum, this means the following information should be provided: [32]

- Description of the personal data to be processed
- Purpose, nature, extent, duration and scope of processing [33]
- Identity of the PIC
- Existence of the rights of the data subject, and how these can be exercised

To avoid impractical or unnecessarily long CCTV Notices, the use of a layered notice should probably be considered.

What information should be included in a CCTV Policy?

A policy that governs the operations of a CCTV System must include the following: [34]

- legitimate purpose/s of the system
- lawful bases for the data processing the system entails
- regular conduct of PIAs and a regular review of the use of the system
- CCTV notice and placement thereof
- operational details of the CCTV system (e.g., procurement, installation, operation, control, monitoring, maintenance, incident response and reporting, etc.)
- designation of authorized personnel responsible for handling access requests, the monitoring of live feeds, and the day-to-day operation of the system
- procedures for access requests (including requests for copies)
- procedure for handling inquiries and complaints
- retention policy and mode of disposal
- security measures
- procedure for audits on the policy's implementation
- procedure for the regular review and assessment of the policy

Can the deployment and management of a CCTV system be outsourced?

Yes. However, the PIC shall remain responsible for the personal data processed by the system. It must then use contractual or other reasonable means to ensure there are proper safeguards when the processing is outsourced or subcontracted to a PIP.[35]

SECURITY

What kinds of safeguards or security controls can one adopt in relation to one's CCTV system?

Examples of security controls that may be adopted for CCTV systems include:

- Making sure that only authorized personnel are tasked to monitor live CCTV feeds[36]
- Making sure that access to the area where CCTV footage is stored is limited to authorized personnel only[37]
- Using a secure disclosure method such that CCTV data becomes accessible only to the intended recipient[38]
- Maintaining the confidentiality of CCTV footage by asking the requesting party to sign a non-disclosure agreement, and/or prohibiting the capture or recording of the footage during a viewing session[39]
- Using a secure method for copying footage such that the integrity of the footage and any associated metadata are maintained[40]
- Maintaining access logs[41]
- Using contractual or other reasonable means to ensure the cooperation and assistance of PIPs (if any)[42]
- Destroying CCTV footage once it is no longer needed for its declared and specified purpose[43]

One may also refer to NPC Circular 2023-06 (Security of Personal Data in the Government and the Private Sector) for a more detailed guidance from the NPC on what measures to implement when securing data processing systems.

Must PIAs be conducted regularly on CCTV Systems?

The NPC appears to suggest this when it notes that the regular conduct of PIAs should be included in a CCTV Policy.[44]

In another issuance, it also emphasizes that previously assessed controls must be monitored, evaluated, updated, and incorporated as a component of a PIC's privacy program.[45]

When must CCTV footage be subjected to masking?

Masking is the process of obscuring or hiding parts of a video or image in order to prevent it from revealing personal data.[46]

According to the NPC, it is only necessary when *all* of the following conditions are present:

1. the requesting party who received the footage is from the media
2. the footage will be made public for news reporting purposes
3. the footage involves images of other people, and not just the specific person being identified for news reporting purposes

If these conditions are all present, the requesting party must mask the images of the other people before making the footage public.[47]

ACCESS REQUESTS

Who may request access to personal data recorded on a CCTV system?

Any of the following may ask for access to such data:

1. a data subject, or any person whose personal data is recorded on a CCTV system[48]
2. an authorized representative of the data subject,[49] including a parent or legal guardian in the case of minors, or lawful heirs in the case of deceased individuals[50]
3. any third party,[51] as long as their access is justified by an appropriate legal basis

What should a data subject or an authorized representative provide when requesting access to CCTV footage?

A data subject or her authorized representative must present the following:

1. an ID or a similar document that would confirm the identity of the data subject[52]
2. purpose of request—which should not be contrary to law, morals, or public policy[53]
3. sufficient details regarding the requested footage (e.g., specific date, approximate time and location, etc.)[54]

If the request is being made through an authorized representative, the representative must also present the following *additional* documents:

1. an ID or a similar document that would confirm the identity of the authorized representative[55]
2. evidence of proper authorization and supporting documents[56]

What should a third party provide when requesting access to CCTV footage?

That depends on who the requesting party is and other relevant details, like the purpose of the request and/or its legal basis.

For example, if a law enforcement agency is seeking access to CCTV footage in line with its constitutional or statutory functions—particularly, in connection with an ongoing criminal investigation—it must provide a written statement, affirmative declaration, or their equivalent, that establishes the lawfulness of the request. It must also relay its request in accordance with its existing standard operating procedures.

When can an access request be denied?

A request to access CCTV footage may be denied based on the following grounds:

1. the information provided along with the request is incomplete [57]
2. the request is deemed frivolous or vexatious [58]
3. the intended purpose or manner of accessing the footage violates legal, ethical, or public policy standards [59]
4. the request is disproportionate to the stated purpose [60]
5. fulfilling the request would impose an unreasonable burden or expense on the relevant parties [61]
6. the footage is no longer available at the time the request is made [62]
7. disclosure of the footage could jeopardize an ongoing criminal investigation [63]

Can the owner of a CCTV System validly refuse to give a copy of a CCTV footage and insist that the requesting party be only allowed to view the footage?

This seems possible, depending on the surrounding circumstances (e.g., purpose of the request).

According to the NPC, once the requesting party has met all the requirements of a proper access request, a PIC (or its PIP) shall allow access to the requested CCTV footage *either* through viewing *or* by providing it with a copy of said footage, taking into account the stated purpose of the request.[64] It also says that a request to obtain a copy of a CCTV footage may be denied if it is disproportionate to the declared purpose of said request.[65]

Denying a request for a copy of the CCTV footage in this case may be seen to include a request to manually record or capture the CCTV footage during the viewing session, through the use of a video camera or some other recording device.

On the other hand, if the request for a copy of the CCTV footage is being enforced via a subpoena or court order, the PIC will likely have no choice but to comply.

Can the owner of a CCTV System validly refuse to give a copy of a CCTV footage and insist that the requesting party be only given still images?

YES. If the PIC encounters a technical difficulty when providing the requesting party with a copy of the CCTV footage, the NPC says it may provide still images, as an alternative. A sufficient amount of stills must be given in order to cover the duration of the requested footage.[66]

Is there a prescribed period for responding to access requests?

YES.

- In the case of a request to view only:
  Five (5) working days from receipt of the request [67]

- In the case of a request to obtaining a copy of the CCTV footage:
  Fifteen (15) working days from receipt of the request [68]

In the case of a complex request or one that involves numerous footages, a CCTV System owner may use an additional period not exceeding (15) working days in order to respond to the request. [69]

If a data subject requests for access to CCTV footage that contains the images of other persons, is there a need to notify or obtain the consent of those other persons before the request is granted?

Not necessarily. It is possible that there may be another legal basis to justify the sharing or release of the CCTV footage. [70]

For instance, the sharing or release of CCTV footage could be necessary in order for the requesting party to pursue its legitimate interests, or to establish a legal claim against the other persons in the footage.

Can the owner of the CCTV system impose a fee on access requests?

Yes, but only when the requesting party is asking for a copy of the footage. Also, the fee has to be reasonable, sufficient only to cover administrative costs. Imposing excessive fees—so as to discourage access requests—is prohibited. [71]

What are the responsibilities of a requesting party once it is given a copy of a CCTV footage?

Once CCTV footage has been released to the requesting party, the latter becomes responsible for its copy of the footage. It must now ensure that it complies with applicable data protection laws and regulations when it processes the CCTV footage as personal data. [72]

RETENTION PERIOD

Is there a recommended retention period for CCTV footages?

None. Two things usually determine the retention period of CCTV footages.

First, there is the law or certain regulations. They sometimes prescribe the exact period within which CCTV footages ought to be preserved. Quezon City, for instance, has an Ordinance requiring covered entities to retain their CCTV footages for at least one (1) year since their recording.[73] The DILG, on the other hand, prescribes a maximum retention period of three (3) weeks.[74]

Second, there is the storage capacity of a CCTV system. In most instances, it is this that determines how long CCTV footages are kept before newer images are written on top of them.

It's important to note, though, that the NPC says the retention period shall not be determined solely by the storage capacity of a CCTV system.[75]

ENDNOTES

[1] NPC Circular 2024-02, second WHEREAS clause; §4(B).
[2] NPC Advisory Opinion 2019-023, p. 2.
[3] NPC Advisory Opinion 2021-032, p. 2.
[4] NPC Advisory Opinion 2020-046, p. 3.
[5] *see*: DPA, §3(l).
[6] NPC Circular 2024-02, §1(A).
[7] NPC Circular 2024-02, §2(G).
[8] NPC Circular 2024-02, §1(A).
[9] NPC Circular 2024-02, §2(E).
[10] NPC Circular 2024-02, §2(E).
[11] NPC Circular 2024-02, §1(A).
[12] NPC Circular 2024-02, §2(G).
[13] NPC Circular 2024-02, §1(A).
[14] *see*: https://www.airbnb.com/help/article/3061
[15] NPC Circular 2023-06, §1(A)
[16] NPC Circular 2024-02, §15.
[17] NPC Circular 2024-02, §12.
[18] *see*: NPC Circular 2022-01, §2.
[19] *see*: DPA, §7(b).
[20] NPC Circular 2024-02, §4(A).
[21] NPC Circular 2024-02, §4(A).
[22] NPC Circular 2024-02, §5(B)(1)(a).
[23] NPC Circular 2024-02, §5(B)(1).
[24] NPC Circular 2024-02, §5(B)(1)(b).
[25] NPC Circular 2024-02, §5(B)(1)(c).
[26] NPC Circular 2024-02, §5(B)(2).
[27] *see*: DILG Memorandum Circular 2022-060, §4.2.
[28] NPC Circular 2023-06, §5.
[29] NPC Circular 2024-02, §5(A)(3).
[30] NPC Circular 2024-02, §5(B)(5).
[31] NPC Circular 2024-02, §3(A).
[32] NPC Circular 2023-04, §3(A).
[33] *see also*: NPC Circular 2024-02, §3(A)(3).
[34] NPC Circular 2024-02, §5(A).
[35] NPC Circular 2024-02, §3(E). See also: NPC Circular 2024-02, §5(B)(6).
[36] NPC Circular 2024-02, §5(B)(3)(c).
[37] NPC Circular 2024-02, §5(B)(3)(a).
[38] NPC Circular 2024-02, §7(A)(2).
[39] NPC Circular 2024-02, §8(B)(1)(c).
[40] NPC Circular No. 2024-02, §8(B)(2)(a).
[41] NPC Circular No. 2024-02, §5(B)(3)(b).
[42] NPC Circular No. 2024-02, §5(B)(6).
[43] NPC Circular No. 2024-02, §5(B)(4)(c).
[44] NPC Circular No. 2024-02, §5(A)(3).

[45] NPC Circular No. 2023-06, §4(D).
[46] NPC Circular No. 2024-02, §2(C).
[47] NPC Circular No. 2024-02, §7(B)(4)(c).
[48] NPC Circular No. 2024-02, §6.
[49] NPC Circular No. 2024-02, §6(A)(3).
[50] *see*: DPA, §17.
[51] NPC Circular No. 2024-02, §7.
[52] NPC Circular No. 2024-02, §6(A)(2).
[53] NPC Circular No. 2024-02, §6(A)(4).
[54] NPC Circular No. 2024-02, §6(A)(5).
[55] NPC Circular No. 2024-02, §6(A)(3).
[56] NPC Circular No. 2024-02, §6(A)(3).
[57] NPC Circular No. 2024-02, §10(A)(1).
[58] NPC Circular No. 2024-02, §10(A)(2).
[59] NPC Circular No. 2024-02, §10(A)(3).
[60] NPC Circular No. 2024-02, §10(A)(4).
[61] NPC Circular No. 2024-02, §10(A)(5).
[62] NPC Circular No. 2024-02, §10(A)(6).
[63] NPC Circular No. 2024-02, §10(A)(7).
[64] NPC Circular No. 2024-02, §8(B).
[65] NPC Circular No. 2024-02, §8(A)(4).
[66] NPC Circular No. 2024-02, §8(B)(2)(b).
[67] NPC Circular No. 2024-02, §9(A).
[68] NPC Circular No. 2024-02, §9(A).
[69] NPC Circular No. 2024-02, §9(B).
[70] NPC Circular No. 2024-02, §6(B).
[71] NPC Circular No. 2024-02, §8(B)(2)(c).
[72] NPC Circular No. 2024-02, §7(A)(1).
[73] QC Ordinance No. SP-2695, S-2018, §3.
[74] DILG Memorandum Circular 2022-060, §4.4.2.
[75] NPC Circular No. 2024-02, §5(B)(4)(a).

REFERENCE MATERIALS

NPC Circulars

- NPC Circular No. 2023-06 (Security of Personal Data in the Government and the Private Sector)
- NPC Circular No. 2022-01 (Guidelines on Administrative Fines)

NPC Advisories

NPC Advisory No. 2020-04 (Guidelines on the Use of Closed-Circuit Television Systems)

NPC Advisory Opinions

- NPC Advisory Opinion No. 2021-032 (Disclosure of photographs of accused in criminal cases)
- NPC Advisory Opinion No. 2020-046 (Common practices of schools in processing personal data of students)
- NPC Advisory Opinion No. 2019-023 (Processing of CCTV footage under the Data Privacy Act of 2012)
- NPC Advisory Opinion No. 2018-080 (Viewing and/or release of CCTV footage)
- NPC Advisory Opinion No. 2018-053 (Photographs and CCTV footages in hospitals)

Other Laws and Regulations

- DILG Memorandum Circular No. 2022-060
- QC Ordinance No. SP-2695, S-2018
- Republic Act No. 10173 (Data Privacy Act of 2012)

PRIVACY.PH

https://www.facebook.com/groups/privacy.ph