DIVINALAW
Enrique Dela Cruz
Senior Partner

Jay-R C. Ipac
Junior Partner

Terence Mark Arthur S. Ferrer
Senior Associate

Scope. The Data Privacy Act or R.A. 10173 applies to processing of all types of personal information and any natural or juridical person involved in processing of said personal information. These entities may be personal information controllers or processors. Moreover, the DPA has extraterritorial applications to personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to exceptions stated in Section 4 of the said Act.

Definition and Types of Personal Information. Personal information refers to "any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."[1] The DPA also distinguishes personal information and sensitive personal information (i.e. age, ethnic origin, marital status, color, religious, philosophical and political affiliations, individual's health, education, genetic or sexual life, offenses committed or alleged, government issued identification, health records, tax returns etc.). Meanwhile, privileged information under the Rules of Court, i.e., information disclosed during the subsistence of a particular professional relationship, e.g., attorney-client relationship, is treated as sensitive personal information.

Governing Principles. Processing refers to "any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data."[2]

Personal information may be processed so long as the requirements under Sections 11 and 12 (if ordinary personal information) and/or 13 (if sensitive personal information) of the

[1] Section 3 (g), R.A. 10173.
[2] Section 3 (j), R.A. 10173.

DPA are complied with. Under Section 11, the processing should adhere to the principles of transparency, legitimate purpose and proportionality. On one hand, Section 12 states that processing is permitted as long as it is not prohibited by law and at least one of the conditions therein exists, e.g., consent of the data subject, necessary for the fulfilment of the contract, or necessary to comply with legal obligations.[3] On the other hand, under Section 13 processing sensitive personal information is generally prohibited unless the data subject has given his or her consent, allowed by existing laws and regulations, necessary to protect the life and health of the data subject or another person in instances where the former cannot express his or her consent, necessary to achieve the lawful and non-commercial objectives of public organizations and their associations, necessary for purposes of medical treatment and necessary for the protection of lawful rights and interest of natural or legal persons in court proceedings or the establishment, exercise or defense of legal claim or when provided to government or public authority.

As consent is a common ground for processing for both personal and sensitive personal information, most recently, the NPC clarified in NPC Circular No. 2023-04 how consent of the data subject should be given. It emphasized the following elements of consent: freely given (i.e., no element of pressure, intimidation, possibility of adverse consequences for refusal to give consent or any other inability to exercise free will by the subjects; see also NPC Advisory No. 2023-01 for Guidelines on Deceptive Design Patterns), specific (i.e., vague or blanket consent is prohibited, and where processing is necessary for the provisions of goods or services then that processing should be disclosed to enable data subject to consent thereto), informed (mandating the controller to minimize risk of consent fatigue), and an indication of will (i.e., implied or inferred consent is not valid; however, continued use of service is consent).

Rights of Data Subjects. Under Section 16 of the DPA, the data subject is provided with the following rights:

(i) right to be informed of processing of personal information including the existence of automated decision-making and profiling. This right includes the right to know to whom his or her personal information is sold or disclosed[4] and right to know the contents of his personal information that were processed;[5]
(ii) right to access;
(iii) right to object to the processing;
(iv) right to erasure or blocking;

[3] See NPC Advisory Opinion No. 2020-50 for more discussions on legitimate interest.
[4] Section 16 (b) (4), R.A. 10173.
[5] Section 16 (c) (3), R.A. 10173.

(v) right to damages;
(vi) right to file a complaint, subject to the requirement of exhaustion and timeliness;
(vii) right to rectify; and
(viii) right to data portability.

Data Protection Officers. A Personal Information Controller must appoint a Data Protection Officer who shall be accountable for compliance under the DPA.

Registration. DPA Implementing Rules and Regulations mandate registration of personal data processing systems of organizations:

(i) If sensitive personal information of at least 1,000 individuals is processed;
(ii) If the personal information controller or processor employs at least 250 persons;
(iii) If less than 250 persons are employed but the processing is not occasional; or
(iv) If less than 250 persons are employed but the processing of the information might pose a risk to the rights and freedoms of the data subject.

Transfer. The Personal Information Controller remains responsible for personal information transmitted to third parties.

Breach. The Personal Information Controller or Processor is required to notify the NPC and the affected data subject of a personal data breach within 72 hours from its discovery.[6]

Relevant Updates. The following are up-to-date applications of the DPA:

Guidelines on the Processing of Personal Data Collected using Body-worn Cameras. NPC Circular No. 2025-01 covers the use of Body-Worn Cameras (BWCs) and alternative recording devices (ARDs) for commercial gain or profit, security and/or law enforcement activities in accordance with the principles of lawful basis for processing, transparency, and fairness. The Circular clarified that Vloggers who use BWCs or ARDs to capture the image, audio, or video of persons for uploading, posting, publishing, or otherwise sharing online may be deemed to be engaged in the processing of personal data and should ensure that such activities are undertaken in a fair and lawful manner. In particular, the Circular required vloggers to (i) ensure transparency and provide adequate information to the data subjects prior to the commencement of any video recording activity, including the fact that the resulting footage will be uploaded, posted, published or otherwise shared online, and how they may exercise their data privacy rights; (ii) to have an appropriate privacy notice on all online platforms which shall provide details to affected data subjects on how to exercise their right to object, right to erasure, take down of posts, among others; and (iii) to use available technology that can mask images of bystanders, especially children and other vulnerable individuals.

[6] Section 20 (4) (f), R.A. 10173.

Considerations on the Use of Privacy-Enhancing Technologies (PET) in the Insurance Industry. NPC and Insurance Comision released a Joint Advisory No. 2025-001 requiring insurance providers, insurance and pre-need companies, health maintenance organizations (HMO), mutual benefit associations (MBA), their respective agents, brokers, adjusters, intermediaries, all other entities under the regulatory control and supervision of the IC to adhere to data privacy laws and regulations and to conduct Privacy Impact Assessments before adoption of PETs.

Child-Oriented Transparency. NPC Advisory No. 2024-03 requires PICs, under the Principle of Transparency, to present any information and communication relating to the processing of personal data in an easy-to-access, concrete, and definitive manner - easily understood by children, and presented in a simple manner using clear and plain language while retaining necessary technical terms. Said NPC Advisory incorporates Child Privacy Impact Assessments within the traditional PIAs, and requires an age assurance mechanism and risk-based approach to determine and implement appropriate and enhanced privacy controls.

Guidelines on Deceptive Design Patterns. NPC Circular No. 2023-01 requires PICs to ensure transparency in the presentation of information to the data subject by avoiding deceptive design pattern and to ensure that personal data is processed in a manner that is neither manipulative nor unduly oppressive to a data subject – by prohibiting the use of deceptive design patterns on analog or digital interfaces, which may result in vitiating the consent of the data subject.

Artificial Intelligence. Under NPC Circular No. 2022-04, a Data Processing System processing personal or sensitive personal information involving automated decision-making or profiling shall, in all instances, be registered with the Commission.[7] In relation thereto, ChatGPT or any other similar AI technology are covered by the Data Privacy Act as the said software requires web scraping of vast bodies of information which includes personal data. Even the NPC emphasizes that "it is a misconception that publicly accessible personal data can be further used or disclosed for any purpose whatsoever without regulation."[8] NPC clarified that marketers, which may corollary include AI technology providers, become personal information controllers of personal information of potential clients obtained from publicly available sources.

In 2021, the Department of Trade and Industry launched the country's Artificial Intelligence (AI) Roadmap which contains four major dimensions for AI readiness, namely: (1) Digitization and Infrastructure, (2) Research and Development, (3) Workforce Development, and (4) Regulation. These dimensions are then supported by seven (7) measurable strategic imperatives and forty-two (42) strategic tasks. In line with this, in

[7] Section 5, NPC Circular No. 2022-04.
[8] Advisory Opinion 2018-050

2022, the country has enacted Republic Act No. 11927, the Philippine Digital Workforce Competitiveness Act and Republic Act 11899, the Second Congressional Commission on Education Act II, to enhance the skills and competitiveness of the Philippine workforce in human, and digital technology and innovations. Recently, House Bill No. 7396 was filed last 1 March 2023 which aims to create an Artificial Intelligence Development Authority (AIDA) which will develop and implement the National AI Development and Regulation Strategy.

Identification Cards. Under NPC Circular No. 2023-03, all personal information controllers issuing ID cards shall ensure that only the necessary personal data are indicated therein in relation to the primary purpose of identifying the data subject.

Customer and Visitor Information. Under NPC Circular No. 2022-03, all personal information controllers, may, through their employed private security agency, collect the visitor's personal information, including visually inspecting their government issued IDs, as long as the data subjects have been sufficiently informed the relevant details regarding the processing via a privacy notice, the collected data is reasonable and proportional to its intended purpose, and adequate safeguards are imposed to protect said data.

Employee Surveillance. Under NPC Advisory Opinion No. 2018-084, monitoring employees' activities in company-issued computers "may be allowable under the DPA, provided the processing falls under any of the criteria for lawful processing of personal data under Section 12 and/or 13 of the law." Moreover, every employer conducting computer monitoring or employee monitoring should ensure that the data collected directly satisfies the purpose of monitoring and that it clearly aligns with the needs and objectives of the organization" without being excessive.

Moreover, NPC PHE Bulletin No. 14 later clarified that work monitoring software may be installed in company-issued devices but employers are required to notify employees of the existence of such software, to conduct a privacy impact assessment to determine risks and mitigation procedures, and to use less privacy-intrusive means of monitoring employees. To elaborate, the means of monitoring should only be proportional to the intended purpose. Thus, requiring employees to stay on video while working is considered excessive. The means of monitoring should be "adequate, relevant, suitable and necessary, and not excessive."