ABLI-FPF CONVERGENCE SERIES

Philippines

Status of Consent for Processing Personal Data

ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

JULY 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTORS

JJ Disini

Managing Partner, Disini Law

Maria Ofelia S. Leaño

Special Counsel, Disini Law

ACKNOWLEDGEMENTS

This Report benefitted contributions and editing support from Elizabeth Santhosh and Catherine Shen.

DISCLAIMER

Views expressed in this Report are not necessarily those of the Project Lead, the Asian Business Law Institute (ABLI), the Singapore Academy of Law (SAL), or the Future of Privacy Forum (FPF). While every effort has been made to ensure that the information contained in this Report is correct, the Authors, the Project Lead, ABLI, SAL, and FPF disclaim all liability and responsibility for any error or omission in this Report, and in respect of any thing, or the consequences of any thing, done or omitted to be done by any person in reliance, whether wholly or partially, upon the whole or part of the consequences of this Report.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Republic Act 10173 – Data Privacy Act of 2012 ("DPA")

The DPA[1] is the main personal data protection legislation in the Philippines and, among other things, governs processing of personal data, which the DPA defines as "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] This broad definition encompasses the collection, processing, and sharing of personal data.

The DPA prescribes distinct requirements for the processing of personal information[3] and sensitive personal information.[4] Consent functions as one of several legal bases for processing both classes of personal data information,[5] subject to the principles of transparency, legitimate purpose, and proportionality, and other laws allowing disclosure of information to the public.[6]

1.2. Implementing Rules and Regulations of the Data Privacy Act of 2012 ("IRRs")

Though the DPA was signed into law in August 2012 and technically took effect in September 2012, there was a transitionary period of one year from the date that the IRRs took effect (i.e., until September 8, 2017[7]) before entities were required to comply with the DPA's requirements.[8]

The stated policy aim of the IRRs[9] is to enforce the DPA and adopt generally accepted international principles and standards for personal data protection, safeguarding individuals' fundamental human right to privacy while ensuring free flow of information for innovation, growth, and national development. [10]

2. SECTORAL LAWS AND REGULATIONS

2.1. Healthcare

The Health Privacy Code of the Philippines[11] ("**Health Privacy Code**") is a set of rules issued by the Department of Health ("**DOH**"), the Department of Science and Technology ("**DOST**"), and the Philippine Health Insurance Corporation ("**Philhealth**") and applies to the Philippine Health Information Exchange ("**PHIE**") system, and to any natural or juridical person involved in the processing of health information within the PHIE framework.

[1] Available at https://www.privacy.gov.ph/data-privacy-act/

[2] DPA, s 3(j).

[3] DPA, s 12.

[4] DPA, s 13.

[5] DPA, ss 12(a) and 13(a).

[6] DPA, s 11.

[7] Per NPC Advisory Opinion No. 2017-17, the IRRs took effect on September 9, 2016, i.e., 15 days from the date that the IRRs were published online in the Official Gazette (August 25, 2016).

[8] DPA, s 42.

[9] Available at https://www.privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/

[10] IRRs, s 2.

[11] Note that the Health Privacy Code (available at: http://www.ehealth.doh.gov.ph/images/HealthPrivacyCode.pdf) was issued in relation to the Philippine Health Information Exchange which was implemented under DOH-DOST-PhilHealth Joint Administrative Order No. 2016-0001, series of 2016 entitled "Implementation of the Philippine Health Information Exchange" (available at http://www.philcancer.org.ph/wp-content/uploads/2016/03/joint_ao_2016-0001_implentation_of_the_phie-1.pdf).

Rule 1 (Collection and Processing of Health Information) of the Health Privacy Code outlines the requirements for valid informed consent for collection and processing of health information, who may give and obtain consent, the form that consent may take, revocation and reinstatement of consent, and exceptions to the requirement to obtain consent.

By default, health information processed in the PHIE must be de-identified, leaving only such information as is necessary for immediate statistical reference. However, a patient's consent functions as an exception to this requirement.

Under Rule 2.1 of the Health Privacy Code, a patient's consent is also necessary for a health care provider and authorized entity to access the patient's health information.

Under Rule 3 of the Health Privacy Code, use and disclosure of health information shall be limited to that covered by the consent given by the patient, or his or her authorized representative, and shall only be for the following purposes:

- planning of quality services;
- reporting of communicable, infectious, and other notifiable diseases, including those that pose a serious health and safety threat to the public, including but not limited to:
    - meningitis;
    - food poisoning (mass);
    - breakthrough epidemic of contagious disease;
    - biological or chemical warfare;
    - emerging and re-emerging diseases;
- continuing care to patients;
- reporting of physical injury;
- reporting of interpersonal violence to proper authorities;
- reporting of diseases as registered in the Philippine Integrated Diseases Surveillance and Response; and
- mandatory reporting required by licensing and accreditation bodies (e.g., DOH, Philhealth, Department of Interior and Local Government, Department of Social Welfare and Development, etc.).

2.2. Health-related research

The National Ethical Guidelines for Health and Health-Related Research[12] provide general guidelines for ethical review of health research (including research involving human participants) and the special guidelines on specific research areas, methodology, and populations.[13] The Guidelines regard informed consent as a core element of research ethics and define such consent as a decision of a competent potential participant to be involved in research after receiving and understanding relevant information, without having been subjected to coercion, undue influence, or inducement.[14] The Guidelines also provide guidance on acquiring informed consent, the essential information that should be provided to the participants of the research, and documenting and renewing consent and waiver of consent.[15]

[12] Available at https://ethics.healthresearch.ph/index.php/phoca-downloads/category/4-neg.

[13] National Ethical Guidelines for Health and Health-Related Research, page 1.

[14] National Ethical Guidelines for Health and Health-Related Research, page 11.

[15] National Ethical Guidelines for Health and Health-Related Research, pages 11-17.

3. ROLE OF THE NATIONAL PRIVACY COMMISSION ("NPC")

Chapter II of the DPA establishes the National Privacy Commission ("**NPC**") – an independent body with a mandate to administer and implement the DPA and to monitor and ensure compliance with international data protection standards.[16] Broadly, the NPC is responsible for, and is given certain powers for the purpose of, rulemaking,[17] advising on matters relating to personal data protection,[18] public education,[19] monitoring compliance with the DPA,[20] investigating and adjudicating on complaints on matters relating to personal data protection,[21] and enforcing compliance with the DPA.[22]

3.1. Advisories

The DPA empowers the NPC to publish, on a regular basis, guides to laws relating to data protection.[23] To that end, the NPC has issued a total of 15 Advisories (including amendments to Advisories)[24] since 2017. These Advisories provide guidelines for complying with the requirements of the DPA as well as best practices for data protection on specific topics, including, among others, designation of data protection officers, conducting privacy impact assessments, using closed-circuit television (CCTV) systems, and upholding data subject rights.

3.2. Advisory Opinions

The DPA also empowers the NPC to issue "Advisory Opinions" which provide NPC's interpretation of the DPA and IRRs and consider the application of these and other relevant laws to specific fact scenarios, often in response to inquiries from the public. As of the date of this Report, NPC has published 307 Advisory Opinions on its website.[25]

4. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE DPA

Consent is one of several legal bases for processing of both non-sensitive and sensitive personal information under the DPA.[26] Although there is no statutory preference for consent over the other bases, in practice, consent has become the *de facto* primary legal basis for processing of personal information because, unlike the other legal bases which apply only in specific contexts, consent is capable of justifying processing of personal data in any context.

Neither the NPC nor any other government body in the Philippines has publicly called for the reconsideration of consent requirements for processing of personal information.

Whether personal information is collected pursuant to consent or another legal basis, the DPA requires that such collection must be for a specified and legitimate purpose, which must be determined and

[16] DPA, s 7. See also IRRs, Rule III.

[17] IRRs, s 9(a).

[18] IRRs, s 9(b).

[19] IRRs, s 9(c).

[20] IRRs, s 9(d).

[21] IRRs, s 9(e).

[22] IRRs, s 9(f).

[23] DPA, s 7(g).

[24] Including amendments to previous Advisories. See https://www.privacy.gov.ph/advisories/

[25] DPA, s 7(l). See https://www.privacy.gov.ph/advisory-opinions/ Note that although the only 307 Advisory Opinions appear on NPC's website, there are

[26] DPA, ss 12(a) and 13(a).

declared before, or as soon as reasonably practicable after, the personal information is collected.[27] Any subsequent processing of personal information that has been collected must also be compatible with such a purpose.[28]

5. Conditions for consent

5.1. Definition and forms of consent

The DPA defines the "consent of the data subject" as any freely given, specific, and informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him/her.[29]

In line with this provision, the NPC has provided further guidance that implied, implicit, or negative forms of consent are not recognized under the DPA.[30]

Consent for processing of sensitive personal information is held to a stricter standard as the DPA requires that such consent must be "specific to the purpose"[31] and obtained prior to collection.[32] By contrast, consent for non-sensitive personal information may be obtained either prior to collection of personal information or as soon as practicable or reasonable thereafter.[33]

Consent must be evidenced by written, electronic, or recorded means.[34] In this respect, the NPC has provided guidance that it has no preference as to whether consent is evidence by written, electronic, or other recorded means.[35]

Lastly, consent may be also given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.[36]

5.2. Withdrawal of consent

The DPA is silent on whether consent may be withdrawn. By contrast, the IRRs expressly provide that consent may be withdrawn[37] and that the data subject has a right to withdraw consent.[38] When the data subject withdraws consent, the data subject may also exercise his/her right to suspend, withdraw or order the blocking, removal or destruction of his/her personal data from the personal information controller's filing system, if there is no other legal ground or overriding legitimate interest for the processing.[39]

The IRRs also require that a data subject should be notified and given an opportunity to withhold consent to processing in case of changes or any amendment to the information supplied or declared to the data subject pursuant to the data subject's right to be informed.[40] When a data subject withholds consent, the personal information controller shall no longer process the personal data, unless:

[27] DPA, s 11(a).
[28] DPA, s 11(a).
[29] DPA, s 3(b).
[30] NPC Advisory Opinion No. 2017-007, page 2, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-007.pdf
[31] DPA, s 13(a).
[32] DPA, s 13(a).
[33] IRRs, s 21(a).
[34] IRRs, s 21(a).
[35] NPC Advisory Opinion No. 2017-007, page 2.
[36] IRRs, s 21(a).
[37] IRRs, s 19(a)(1).
[38] IRRs, s 19(a)(1).
[39] IRRs, s 34(e)(1)(d). See also DPA, s 16(e).
[40] IRRs, s 34(b). As to the right to be informed, see DPP, s 16(a) and IRRs, s 34(a).

- the personal data is needed pursuant to a subpoena;[41]
- the collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject;[42] or
- the information is being collected and processed as a result of a legal obligation.[43]

5.3. Bundled consent

The DPA and IRRs are silent as to "bundled consent." However, it appears that such a practice would be inconsistent with the DPA's definition of consent as a "freely given, specific, and informed indication of will."[44] In NPC Advisory Opinion No. 2018-013, the NPC opined that bundled consent "will generally not suffice as the data subject is not empowered to make a true choice."[45] NPC reiterated this opinion in NPC Case No. 19-910 dated 17 December 2020 (*In Re: FLI Operating ABC Online Lending Application*).

The DPA does not specifically prohibit a controller from blocking access by a data subject to services should the subject refuse to give consent to the processing of their personal data.

6. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

The DPA distinguishes between personal information, sensitive personal information, and privileged information.[46]

The DPA defines sensitive personal information as personal information:

- about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;[47]
- about an individual's health, education, genetic or sexual life, or any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;[48]
- issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns;[49] and
- specifically established by an executive order or an act of Congress to be kept classified.[50]

Processing of sensitive personal information is prohibited, except where the data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing[51] or where another legal basis under Section 13 of the DPA exists.

[41] IRRs, s 34(b)(1).
[42] IRRs, s 34(b)(2).
[43] IRRs, s 34(b)(3).
[44] DPA, s 3(b).
[45] NPC Advisory Opinion No. 2018-013, page 3, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AdOpNo.2018-013.pdf
[46] DPA, s 13.
[47] DPA, s 3(l)(1).
[48] DPA, s 3(l)(2).
[49] DPA, s 3(l)(3).
[50] DPA, s 3(l)(4).
[51] DPA, s 13(a).

However, in practice, consent would almost always be required for the processing of sensitive personal information as the other legal bases for processing sensitive personal information apply only in narrow circumstances. There are also heavier penalties associated with the unauthorized processing or mishandling of sensitive personal information (see below).

“Privileged information” is subject to the same treatment as sensitive personal information.[52] Privileged information refers to any and all forms of data which would constitute privileged communication under the Philippines’ Rules of Court or other pertinent laws.[53]

6.1. Children

The DPA does not specifically address the issue of children’s consent. However, the NPC has opined that a minor cannot validly provide consent as defined under the DPA.[54] Note that the age of majority in the Philippines is 18.

6.2. Cookies, Internet of Things, online tracking

The DPA does not address cookies, Internet of Things, and online tracking. However, note that the NPC has opined that IP addresses, MAC addresses, and cookies (among others) would qualify as personal information, but not sensitive personal information, under the DPA.[55]

6.3. Direct marketing

The DPA defines direct marketing as “communication by whatever means of any advertising or marketing material which is directed to particular individuals”[56] but does not contain any specific provisions providing protection for personal information that is or is to be used in direct marketing.

Rather, such provisions are found in the IRRs, which require that where personal information is to be processed for direct marketing, the data subject must be provided with specific information regarding the purpose and extent of such processing.[57] The IRRs also expressly provide data subjects with a right to object to processing of their personal information for direct marketing purposes – data subjects must therefore be notified if their personal information will be used for such purposes and be given an opportunity to withhold consent.[58]

The IRRs further require that data sharing for commercial purposes, including direct marketing purposes, must be covered by a data sharing agreement which establishes adequate safeguards for data privacy and security and upholding data subjects’ rights[59] and is subject to review by the NPC. [60]

Lastly, in NPC Advisory Opinion No. 2017-051, the NPC opined that when an *employee’s* personal data is used for marketing purposes, consent is required since its use is neither necessary nor related to an employer-employee contract.[61]

[52] DPA, s 13.

[53] DPA, s 3(k).

[54] NPC Advisory Opinion No. 2017-049, page 3, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-049.pdf

[55] NPC Advisory Opinion No. 2017-063, page 3, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-063.pdf

[56] DPA, s 3(d).

[57] IRRs, ss 19(a)(2) and s 34(a)(2)(b).

[58] IRRs, s 34(b).

[59] IRRs, s 20(b)(2)(a).

[60] IRRs, s 20(b)(2)(b).

[61] NPC Advisory Opinion No. 2017-051, page 3, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-051.pdf

6.4. Biometric and genetic data

The DPA's definition of sensitive personal information expressly refers to genetic information.[62] The status of biometric data is less clear – in so far as specific biometric data identifies a person's race, ethnic origin, age, color, or genetics, it would likely qualify as sensitive personal information under the DPA.

6.5. Financial information

Generally, financial information would qualify as personal information under the DPA. However, note that the DPA does not apply to information that is necessary for banks and other financial institutions to comply with certain anti-money laundering laws.[63]

6.6. Statistics and research

The processing of data for research purposes is specifically exempted from the scope of the DPA.[64] However, the IRRs have narrowed the scope of this exemption so that it now applies only to research for a public benefit.[65] Notably, the IRRs also state that the NPC may, on its own initiative or upon the filing of a complaint by a data subject, review processing for research purposes.[66]

6.7. Pseudonymized data

The DPA does not expressly address pseudonymization of data. However, in NPC Advisory Opinion No. 2018-029, the NPC opined that pseudonymized personal data remains personal data and so, in principle, would require a legal basis for processing under the DPA.[67] The NPC took the view that if an entity is in possession of information that allows it to identify data subjects whose personal information has been pseudonymized, then the information would qualify as personal information.

The treatment, however, is different in the case of anonymized data or de-identified personal data. In NPC Advisory Opinion No. 2018-056, the NPC opined that de-identified personal data (as opposed to pseudonymized data) would no longer be considered as personal information as the purpose of de-identification is to remove identifiers so that the remaining information no longer relates to an identified or identifiable person.[68]

6.8. Location data

Regarding location data, the NPC opined that location data qualifies as personal information but not sensitive personal information.[69]

[62] DPA, s 3(l)(2).

[63] DPA, s 4(f).

[64] DPA, s 4(d).

[65] IRRs, s 5(c). See also NPC Advisory Opinion No. 2018-54, page 1, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-054.pdf

[66] IRRs, s 49(e).

[67] NPC Advisory Opinion No. 2018-029, page 2, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AdOpNo.2018-029.pdf

[68] NPC Advisory Opinion No. 2018-056, page 3, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-056.pdf

[69] NPC Advisory Opinion No. 2017-063, page 3, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-063.pdf

7. CONSENT FOR CROSS-BORDER DATA TRANSFERS

Cross-border data transfers qualify as a form of “processing” pursuant to Section 3(j) of the DPA and accordingly, would require the data subject’s consent or fulfillment of another legal basis for processing.

Unlike other data protection laws internationally, the DPA does not specifically prohibit cross-border data transfer but rather, operates on an accountability framework. A personal information controller is responsible for personal information under its control or custody, including information that has been transferred internationally to a third party for processing, and must use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.[70]

8. TRANSPARENCY AND NOTICE

8.1. DPA

As discussed above, the DPA requires consent to be informed[71] and the purpose of processing to be declared before, or as soon as reasonably practicable, after collection.[72]

Additionally, the DPA provides data subjects with rights, among others, to be informed of whether their personal information will be, is, or has been processed,[73] and to be furnished with the following information before their personal information is entered into the controller’s processing system, or at the next practical opportunity: [74]

- a description of the personal information to be entered into the system;[75]
- purposes for which the personal information is being or is to be processed;[76]
- the scope and method of the personal information processing; [77]
- the recipients or classes of recipients to whom the personal information is disclosed or may be disclosed;[78]
- methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;[79]
- the identity and contact details of the personal information controller or its representative;[80]
- the period for which the personal information will be stored;[81] and
- the existence of the rights of data subjects, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.[82]

[70] DPA, s 21.
[71] DPA, s 3(b).
[72] DPA, s 11(a).
[73] DPA, s 16(a).
[74] DPA, s 16(b).
[75] DPA, s 16(b)(1).
[76] DPA, s 16(b)(2).
[77] DPA, s 16(b)(3).
[78] DPA, s 16(b)(4).
[79] DPA, s 16(b)(5).
[80] DPA, s 16(b)(6).
[81] DPA, s 16(b)(7).
[82] DPA, s 16(b)(8).

8.1. IRRs

The IRRs expand on the principle of transparency in the DPA.

In particular, the data subject must be made aware of the nature, purpose, and extent of the processing of his/her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised.[83]

Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.[84]

9. SANCTIONS AND ENFORCEMENT

9.1. Criminal liability

The DPA prescribes the following offenses for breach of consent provisions:

a. Unauthorized processing of personal and sensitive personal information

A person who processes personal information without the consent of the data subject or another lawful basis face imprisonment for 1 to 3 years and a fine of between PHP 500,000.00 and PHP 2,000,000.00.[85]

A person who processes sensitive personal information without the consent of the data subject or another lawful basis faces imprisonment for 3 to 6 years and a fine of between PHP 500,000.00 and PHP 4,000,000.00.[86]

b. Processing of personal information for unauthorized purposes

A person who processes personal information for purposes not authorized by the data subject or by law face imprisonment for 1.5 to 5 years and a fine of between PHP 500,000.00 and PHP 1,000,000.00.[87]

A person who processes sensitive personal information for purposes not authorized by the data subject or by law face imprisonment for 2 to 7 years and a fine of between PHP 500,000.00 and PHP 2,000,000.00.[88]

c. Malicious and unauthorized disclosures

Any personal information controller or personal information processor or any of its officials, employees, or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information faces imprisonment for 6 months to 5 years and a fine of between PHP 500,000.00 and PHP 1,000,000.00.[89]

Any personal information controller or personal information processor or any of its officials, employees, or agents, who disclose to a third party personal information not covered by the above paragraph without the consent of the data subject face imprisonment ranging from 1 to 3 years and a fine of between PHP 500,000.00 and PHP 1,000,000.00.[90]

[83] IRRs, s 18(a).
[84] IRRs, s 18(a).
[85] DPA, s 25(a); IRRs, s 52(a).
[86] DPA, s 25(b); IRRs, s 52(b).
[87] DPA, s 28(a); IRRs, s 55(a).
[88] DPA, s 28(b); IRRs, s 55(b).
[89] DPA, s 31; IRRs, s 58.
[90] DPA, s, 32(a); IRRs, s 59(a).

Additionally, if sensitive personal information is disclosed, the possible term of imprisonment increases to 3 to 5 years and a fine of between PHP 500,000.00 and PHP 2,000,000.00.[91]

A person who is found to have committed a combination or a series of acts discussed above shall be subject to imprisonment ranging from 3 to 6 years and a fine of not less than PHP 1,000,000.00 but not more than PHP 5,000,000.00.[92]

9.2. Civil liability

A data subject is entitled to be indemnified for any damages sustained due to unlawfully obtained or unauthorized use of personal information, among others.[93]

9.3. Enforcement actions

While the NPC does not actively check each entity's compliance with consent provisions and requirements, the NPC is active in acting upon cases and complaints brought to it, including violations of consent provisions and requirements.

The following is a non-exhaustive list of examples of NPC decisions which have enforced consent provisions in the DPA.

a. *BGM v. IPP* (NPC 19-653)[94]

The Respondent was ordered to disclose to the Complainant the identity of one of the merchants on the Respondent's online platform, without the merchant's consent, as the merchant appeared to have defrauded the Complainant, and the Complainant intended to file legal actions against the Merchant.

The NPC found that such disclosure would not constitute unauthorized processing because the Complainant was exercising her right to access by requesting that the Respondent disclose parties to whom the Complainant's personal information has been shared. The NPC also found that disclosure to the Complainant would be covered by the Complainant's legitimate interest in protecting her lawful rights and interests which could not be fulfilled by other means.[95]

b. *In Re: FLI Operating ABC Online Lending Application* (NPC 19-910)[96]

The NPC found that an operator of an online lending application had processed information without the consent of the data subject and without authorization under the DPA or any existing law.

The facts of the case are as follows: (a) data subjects had entered into a credit agreement with the lending company in which data subjects gave consent for the company to "collect, process, and retain" personal information including, among others, data subjects' mobile phone numbers and phone contacts in order to achieve the purpose of an agreement;[97] (b) data subjects clicked "agree" on the lending company's privacy policy, which provided that the data subjects consented to, among others, use and disclosure of their personal information for the same purpose;[98] and (c) the lending company proceeded to access lists of contacts on data subjects' smartphones, and its debt collectors sent messages to these contacts.

[91] DPA, s 32(b); IRRs, s 59(b).

[92] DPA, s 33.

[93] DPA, s 16(f).

[94] NPC's decision in *BGM v. IPP* (NPC 19-653) is available at https://www.privacy.gov.ph/wp-content/uploads/2021/02/NPC-19-653-BGM-vs-IPP-Decision-FINAL-Pseudonymized-21Dec2020.pdf

[95] *BGM v. IPP* (NPC 19-653), page 8.

[96] NPC's decision is available at https://www.privacy.gov.ph/wp-content/uploads/2021/02/NPC-19-910-In-re-FLI-Decision-LYA-Final-pseudonymized-17Dec2020-.pdf

[97] *In Re: FLI Operating ABC Online Lending Application* (NPC 19-910), page 20.

[98] *In Re: FLI Operating ABC Online Lending Application* (NPC 19-910), page 20.

The NPC found that the declared purpose was insufficient to form a basis for informed consent as it was circuitous and overbroad.[99] Collection of data subjects' contacts was also excessive as less intrusive means, such as relying on a limited list of contacts provided by data subjects, were available.[100] Additionally, the NPC found that the privacy policy did not contemplate that the lending company would access data subjects' full contact lists as the privacy policy only referred to personal information "provided by the borrower" to lending company, and data subjects did not specifically provide their contact lists.[101] While the privacy policy referred to "collection purposes," this could not be taken as a blanket authority for excessive collection and unauthorized retention of information.[102]

c. *In Re: Lisensya.Info*[103]

The NPC issued a Cease-and-Desist Order against a website, Lisensya.Info, which presented itself as connected with a regulatory agency, the Land Transportation Office ("**LTO**"). When users entered a license number and birth dates into the website, the website would return the name of the license owner and expiration date of the license. When users entered a motor vehicle file number, the website would reveal the model, plate number, engine number, chassis number, and registration expiry date of the motor vehicle, and the name of the motor vehicle's owner.

The NPC found that the website had unlawfully obtained information from the LTO and processed personal information without the consent of the affected data subject or other legal authorization.[104] As the NPC found that operation of the website was detrimental to the public interest and risked causing grave and irreparable injury to the affected data subjects,[105] the NPC issued a cease-and-desist order to the owner and operator of the website.

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

The DPA recognizes legitimate interests as a lawful basis for processing of personal information. There is no equivalent basis for processing of sensitive personal information.

Specifically, the DPA permits processing of personal data without the data subject's consent where such processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party/parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[106]

A personal information controller or third party who relies on this provision must still comply with the principles of transparency, legitimate purpose, and proportionality under the DPA.[107] The data subject also has the right under Section 16(a)-(b) of the DPA to be informed of such processing and to request for the personal information controller or third party to cease such processing.[108]

The NPC has provided guidance on this basis in a number of Advisory Opinions.

[99] *In Re: FLI Operating ABC Online Lending Application* (NPC 19-910), page 24.

[100] *In Re: FLI Operating ABC Online Lending Application* (NPC 19-910), pages 25-26.

[101] *In Re: FLI Operating ABC Online Lending Application* (NPC 19-910), pages 26 and 30.

[102] *In Re: FLI Operating ABC Online Lending Application* (NPC 19-910), pages 26 and 30.

[103] NPC's decision in *In Re: Lisensya.Info* (12 December 2020) is available at https://www.privacy.gov.ph/wp-content/uploads/2021/01/Cease-And-Desist-Order-Re-In-Re-Lisensya.Info-11-12-20-Pseudonymized-17Dec20-ADJU1.pdf

[104] *In Re: Lisensya.Info*, pages 9 and 11.

[105] *In Re: Lisensya.Info*, at pages 11-12.

[106] DPA, s 12(f).

[107] DPA, s 11.

[108] DPA, s 16(a)-(b); IRRs, s 34(b).

In particular, the NPC has defined a "legitimate interest" as a matter that is desired by or important to the personal information controller.[109] In line with Section 18 of the IRRs, a legitimate interest must not be contrary to law, morals, or public policy.[110]

Citing guidance from the United Kingdom Information Commissioner's Office (ICO), the NPC has also stated that three tests must be satisfied before a legitimate interest may be used as a ground for processing personal information:

- a **purpose test** which establishes the existence of the legitimate interest and determines the objective of the particular processing operation;
- a **necessity test**, which requires that the processing of personal information must be necessary for the purpose pursued by the personal information controller or a third party to whom personal information is disclosed, where such a purpose could not be reasonably fulfilled by other means; and
- a **balancing test**, which requires consideration of the likely impact of processing on the data subject as the legitimate interest must not override the data subject's fundamental rights and freedoms.[111]

The standard applied in the balancing test is reasonableness, and relevant factors to be weighed in the balance would include a reasonable expectation on the part of the data subject at the time and in the context of collection of personal information and the relationship between the personal information controller and the data subject.[112] Further, the NPC has acknowledged that the provisions of the DPA were highly influenced by the European Union's Directive 95/46/EC and that NPC's interpretation of these provisions drew guidance from the recitals to the GDPR.[113]

10.1. Documenting the balancing exercise

Neither the DPA nor the IRRs explicitly require the controller to document the balancing exercise in relation to legitimate interest, or to conduct a Privacy Impact Assessment.

However, the NPC's Guidelines on Privacy Impact Assessments – issued in July 2017 – recognizes that conducting a Privacy Impact Assessment is good practice for every personal information controller or processor.[114]

10.2. Disclosing reliance on the balancing test

A personal information controller must disclose to the data subject that the controller is processing personal information on the basis of a legitimate interest (or any legal basis other than consent).[115]

Reliance on the legitimate interests basis does not require pre-approval or review by the regulator. However, as part of the NPC's function of ensuring compliance with the provisions of the law, the NPC may require the controller to disclose information pertaining to the controller's compliance with its obligations under the DPA.[116]

[109] NPC Advisory Opinion No. 2018-061, page 2, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-061.pdf

[110] NPC Advisory Opinion No. 2018-061, page 2. See also IRRs, s 18(b).

[111] NPC Advisory Opinion No. 2018-061, page 2, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-061.pdf

[112] NPC Advisory Opinion No. 2018-050, page 4, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-050.pdf

[113] NPC Advisory Opinion No. 2018-050, at pages 2-4.

[114] NPC Advisory No. 2017-03, page 4, available at https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC_AdvisoryNo.2017-03.pdf

[115] IRRs, s 34(a)(2)(c).

[116] DPA, s 9(d)(1).

11. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

11.1. Processing non-sensitive personal information

The DPA permits processing of personal information without the data subject's consent where such processing is necessary:

- and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;[117]
- for compliance with a legal obligation to which the personal information controller is subject; [118]
- to protect vitally important interests of the data subject, including life and health;[119]
- in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate;[120] or
- for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[121]

a. Fulfillment of a contract or preparatory steps for entering into a contract

The NPC has provided guidance for purposes of this legal basis. The NPC interprets the term "contract" as any contract defined under the Civil Code.[122] The NPC has also listed some examples of when this basis may be applied or used:

- where an employer processes the personal information of an employee as a consequence of their employer-employee relationship or in contemplation of entering into such a relationship; and
- processing of personal information in relation to services requested by a data subject-depositor from a bank.[123]

11.2. Processing sensitive personal information

The DPA permits processing of sensitive personal information under the following legal bases:

- existing laws and regulations provide for processing of sensitive personal information, provided that:
  - such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information, and
  - the consent of the data subjects is not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;[124]

[117] DPA, s 12(a).
[118] DPA, s 12(c).
[119] DPA, s 12(d).
[120] DPA, s 12(e).
[121] DPA, s 12(f).
[122] NPC Advisory Opinion No. 2017-033, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-033.pdf
[123] NPC Advisory Opinion No. 2017-033.
[124] DPA, s 13(b).

- the processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;[125]
- the processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations, provided that
  - such processing is only confined and related to the *bona fide* members of these organizations or their associations,
  - the sensitive personal information is not transferred to third parties, and
  - consent of the data subject was obtained prior to processing; [126]
- the processing is necessary for purposes of medical treatment carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured;[127] or
- the processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority.[128]

11.3. Exemptions

The DPA, including requirements that personal information may only be processed with a legal basis (such as consent), does not apply with respect to the following:

- information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
  - the fact that the individual is or was an officer or employee of the government institution;[129]
  - the title, business address and office telephone number of the individual;[130]
  - the classification, salary range and responsibilities of the position held by the individual;[131] and
  - the name of the individual on a document prepared by the individual in the course of employment with the government;[132]
- information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;[133]
- information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;[134]
- personal information processed for journalistic, artistic, literary or research purposes; [135]

[125] DPA, s 13(c).
[126] DPA, s 13(d).
[127] DPA, s 13(e).
[128] DPA, s 13(f).
[129] DPA, s 4(a)(1).
[130] DPA, s 4(a)(2).
[131] DPA, s 4(a)(3).
[132] DPA, s 4(a)(4).
[133] DPA, s 4(b).
[134] DPA, s 4(c).
[135] DPA, s 4(d).

- information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions; [136]
- information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; [137] and
- personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines. [138]

a. Research purposes

The DPA expressly excludes research purposes from its scope.[139] However, as stated above, the IRRs have restricted the scope of this exemption to research intended for public benefit, subject to the requirements of applicable laws and regulations.[140] The IRRs also permit the NPC to review processing for research purposes on its own initiative or upon the filing of a complaint by a data subject.[141]

The NPC opined further in Advisory Opinion No. 2018-054 that the research exemption is not absolute but only to the minimum extent necessary to achieve a specific purpose, function, or activity.[142]

The intent of the DPA appears to be to maintain flexibility in processing of personal information for research purposes, in line with the DPA's stated policy goals of protecting the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth and recognizing that information and communication technology plays a vital role in nation-building.[143]

b. Health research

The DPA does not provide specific requirements for processing of personal information for the purpose of health research. However, the DPA provides a general exemption for research which would cover health research for public benefit (see above). The IRRs further provide that processing for research purposes should only be exempted from the DPA's requirements to the minimum extent necessary to achieve the specific purpose, function, or activity[144] and remains subject to the requirements of applicable laws, regulations, and ethical standards.[145]

In this regard, note that Rule 10 of the Health Privacy Code requires the patient's consent for collection of visual images, identifiable information must be removed or obscured, and that participants must be permitted to opt out of research and have their personal information deleted from the project database.

Additionally, for health research and research involving human participants, the National Ethical Guidelines for Health and Health-Related Research provide that informed consent is an essential element of research ethics. These guidelines define informed consent as a decision of a competent

[136] DPA, s 4(e).
[137] DPA, s 4(f).
[138] DPA, s 4(g).
[139] DPA, s 4(d).
[140] IRRs, s 5(c). See also NPC Advisory Opinion No. 2018-54, page 1, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-054.pdf
[141] IRRs, s 49(e).
[142] IRRs, s 5(c). See also NPC Advisory Opinion No. 2018-54, page 1, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-054.pdf
[143] DPA, s 2.
[144] IRRs, s 5.
[145] IRRs, s 5(c).

potential participant to be involved in research after receiving and understanding relevant information, without having been subjected to coercion, undue influence, or inducement.

11.4. Sectoral laws and regulations

a. Credit Information

Under the Republic Act No. 9510 (Credit Information System Act),[146] banks, quasi-banks, their subsidiaries and affiliates, life insurance companies, credit card companies and other entities that provide credit facilities are required to submit to the Central Credit Information Corporation ("**CCIC**") basic credit data and updates, including positive and negative credit data thereon on a regular basis.

The CCIC may also access credit and other relevant information from government offices, judicial and administrative tribunals, prosecutorial agencies, and other related offices.[147] The CCIC is authorized to release consolidated credit data on the borrower to accessing entities, special accessing entities, outsource entities (as defined under the law) and the borrowers.[148]

b. Drug rehabilitation

Under the Comprehensive Dangerous Drugs Act of 2002, the DOH oversees all drug rehabilitation activities as well as privately-owned drug treatment rehabilitation centers and drug testing networks and laboratories throughout the Philippines. The NPC has opined that private drug rehabilitation centers may submit personal information of patients who undergo drug testing to the DOH via the DOH's Integrated Drug Testing Management Information System without the patients' consent.[149]

11.5. Specific circumstances

a. Carrying out a task in the public interest

The DPA does not provide a general legal basis for processing of personal information to carry out a task in the public interest.

However, the DPA permits processing of personal information where necessary to comply with the requirements of public order and safety and to fulfill the functions of public authorities.[150]

Additionally, processing of personal information to perform a task in the public interest would also likely be permitted by the legitimate interests basis, provided that performance of the task is necessary and does not override fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[151]

b. Necessity for law enforcement, defense, or national security

The DPA expressly excludes from its scope personal information necessary to carry out the functions of a public authority, including processing of personal information by law enforcement agencies for performance of their constitutionally and statutorily mandated functions.[152] Such processing would not be subject to requirements for consent or another lawful basis in the DPA. However, note that the IRRs

[146] Available at https://www.creditinfo.gov.ph/republic-act-no-9510-credit-information-system-act-cisa-0
[147] Credit Information System Act, s 4(e).
[148] Credit Information System Act, s 4(g).
[149] NPC Advisory Opinion No. 2018-066, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-066.pdf
[150] DPA, s 12(e).
[151] DPA, s 12(f).
[152] DPA, s 4(e).

clarify that the exemption applies to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned.[153]

Additionally, the DPA permits processing of personal information without consent where necessary to respond to a national emergency, comply with the requirements of public order and safety, or fulfill functions of public authority.[154] There is no equivalent legal basis for processing of sensitive personal information.

c. Necessity for prevention, detection, mitigation, and investigation of fraud, security breach, or other prohibited/illegal activities in high-risk scenarios

The DPA does not provide any specific legal bases for these purposes. However, processing of personal information for these purposes without consent would likely be permitted under the legitimate interests basis, provided that the processing is necessary for these purposes, and these purposes are not overridden by fundamental rights and freedoms of the data subject protected by the Philippine Constitution.[155]

Note that there is no equivalent legal basis for processing of sensitive personal information.

11.6. Rule of interpretation

a. DPA

The DPA provides that any doubt in the interpretation of any provision of the DPA should be interpreted in a manner mindful of the rights and interests of the individual about whom the personal information is processed.[156]

b. Role of IRRs

Case law in the Philippines has established that implementing rules and regulations cannot enlarge, alter, or restrict the provisions of the law they seek to implement.[157]

11.7. COVID-19

The NPC has taken the opportunity to issue several Advisory Opinions where it cited legal bases other than consent in relation to COVID-19. In particular, it has consistently cited processing which is provided for by existing laws and regulations as the legal basis for processing sensitive personal information pertaining to COVID-19.

In NPC Advisory Opinion 2020-022,[158] the NPC expressed the view that the DPA permits DOH, a public authority performing regulatory functions, to process personal data to the extent necessary for the fulfillment of these functions, including conducting disease surveillance, epidemic investigation, contact tracing, survey research, and disease registry.[159] The NPC also stated that it expected contact tracing, which involves processing of both personal and sensitive personal information, to be in accordance with relevant existing laws and regulations, such as Republic Act No. 11332 or the Mandatory Reporting

[153] IRRs, s 5. See also NPC Advisory Opinion No. 2017-020, available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-020.pdf

[154] DPA, s 12(e).

[155] DPA, s 12(f).

[156] DPA, s 38.

[157] *Pilipinas Kao, Inc. v. Court of Appeals*, 423 Phil. 834 [2001].

[158] NPC Advisory Opinion No. 2020-022, available at https://www.privacy.gov.ph/wp-content/uploads/2020/10/Redacted-Advisory-Opinion-No.-2020-022.pdf

[159] NPC Advisory Opinion No. 2020-022, at pages 3-4.

of Notifiable Diseases and Health Events of Public Health Concern Act, as well as the issuances of the DOH.[160]

In NPC Advisory Opinion 2020-028,[161] the NPC also advised that the provision of death certificates, which contain sensitive personal information, to the Department of Interior and Local Government ("**DILG**") constitutes processing, which is provided for by existing laws and regulations, as there are several issuances of the DOH and the DILG on reporting deaths in relation to COVID-19.

Furthermore, NPC issued NPC Advisory No. 2020-03 (the Guidelines for Workplaces and Establishments)[162] processing personal data for COVID-19 Response. These guidelines require establishments to provide a privacy notice to employees, visitors, and clients, and the information to be included in the privacy notice include the legal basis for processing which are the existing laws and regulations of the DOH, Department of Labor and Employment, and the Department of Trade and Industry which require the accomplishment of health declaration forms and contact tracing forms.[163]

[160] NPC Advisory Opinion No. 2020-022, at page 3.

[161] NPC Advisory Opinion 2020-028, available at https://www.privacy.gov.ph/wp-content/uploads/2020/10/Redacted-Advisory-Opinion-No.-2020-028.pdf

[162] Available at https://www.privacy.gov.ph/wp-content/uploads/2020/11/NPC-Advisory-No.-2020-03-FINAL.pdf

[163] NPC Advisory No. 2020-03, s 4(B).

ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005 FPF.ORG | INFO@FPF.ORG