TABLE OF CONTENTS

November 2021

1. GOVERNING TEXTS

1.1. Legislation

The Data Privacy Act of 2012 (Republic Act No. 10173) ('the Act') does not specifically regulate cookies. However, in the National Privacy Commission's ('NPC') Advisory Opinion No. 2017-063 ('the Advisory Opinion 63'), the NPC opined that information acquired from the use of cookies, when combined with other pieces of information, may allow an individual to be distinguished from others and may, therefore, be considered personal information.

The Act applies to the processing of all types of personal information and to any natural and juridical person involved in the processing of such personal information, including those personal information controllers and personal information processors who, although not found or established in the

Philippines, use equipment located in the Philippines, or those who maintain an office, branch, or agency in the Philippines. The use of cookies to collect, use, or otherwise process personal information is within the purview of the Act.

In addition to the Act, the following are laws that generally govern data privacy and protection in the Philippines:

- the Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties therefore and for Other Purposes (Republic Act No. 10175), which prohibits, among other things, offences against the confidentiality, integrity, and availability of computer data, including illegal access, illegal interception, data interference, system inference, and misuse of devices, as well as computer-related offences, such as computer-related forgery, computer-related fraud, and computer-related identity theft;
- the Electronic Commerce Act of 2000 (Republic Act No. 8792), which applies to any kind of data message and electronic document used in the context of commercial and non-commercial activities, including domestic and international dealings, transactions, arrangements, agreements contracts and exchanges, and storage of information; and
- the Access Devices Regulation Act of 1998 (Republic Act No. 8484), which prohibits access device fraud, which includes disclosing any information imprinted on the access device such as, but not limited to, the account number, name or address of the device holder, without the latter's authority or permission.

1.2. Regulatory Authority Guidance

The regulatory authority responsible for the administration and enforcement of the Act is the NPC.

The NPC has issued its Implementing Rules and Regulations of Republic Act No. 10173 ('IRR') to provide the necessary particulars for the enforcement of the Act. It has likewise issued circulars, compliance with which is mandatory, as well as advisories and advisory opinions which, though not binding, are instructive as to the NPC's standards in implementing the Act. This includes its Advisory Opinion No. 2017-47 ('the Advisory Opinion 47').

2. DEFINITIONS

Cookies and similar technologies: There is no definition of cookies and similar technologies in the Act, the IRR, or any NPC issuances.

Consent: Consent is defined in the IRR as a freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his/her personal, sensitive personal, or privileged information. Consent must be evidenced by written, electronic, or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorised by the data subject to do so (Section 3 of the IRR).

3. CONSENT & COOKIE POLICY

General rules on consent

Consent is required prior to the collection and processing of personal data, subject to exemptions provided in law. When consent is required, it must be time-bound in relation to the declared, specified, and legitimate purpose. Consent given may be withdrawn. Furthermore, in obtaining consent, the data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his/her personal data for profiling, processing for direct marketing, and data sharing (Section 19 of the IRR). Specifically, as to data sharing, consent for the same is required even when the data is to be shared with an affiliate or mother company, or similar relationships (Section 20 of the IRR).

As a general rule, in the case of the processing of personal information, the data subject must give his/her consent prior to its collection, or as soon as practicable and reasonable (Section 21 of the IRR). In comparison, when the subject of the processing is sensitive personal information, unless any of the exceptions apply, consent must be given by the data subject prior to the processing. Personal information is 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. Sensitive personal information, on the other hand, refers to personal information (Section 3(d) of the IRR):

- concerning an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical, or political affiliations;
- about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offence committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
- issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licences or their denials,

suspension or revocation, and tax returns; or
- specifically established by an executive order or an act of Congress to be kept classified.

When processing personal information, consent may be dispensed with where (Section 21 of the IRR):

- the processing activity involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfil obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect vitally important interests of the data subject, including his/her life and health;
- the processing of personal information is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law;
- the processing of personal information is necessary for the fulfilment of the constitutional or statutory mandate of a public authority; or
- the processing is necessary to pursue the legitimate interests of the 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 Constitution of the Republic of the Philippines.

When processing sensitive personal information, meanwhile, there is no need to acquire prior consent where (Section 22 of the IRR):

- the processing of sensitive personal information is provided for by existing laws and regulations, provided that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data;
- 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/her consent prior to the processing;
- the processing is necessary to achieve the lawful and non-commercial objectives of public organisations and their associations, provided that:
    - the processing is confined and related to the *bona fide* members of these organisations or their associations;
    - the sensitive personal information is not transferred to third parties; and
    - the consent of the data subject was obtained prior to processing;

- the processing is necessary for the purpose of medical treatment, provided that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured; or
- the processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defence of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

No decision with legal effects concerning a data subject must be made solely on the basis of automated processing without the consent of the data subject (Section 48 of the IRR).

In NPC Advisory No. 21-01, the NPC requires controllers to notify and furnish data subjects with information indicated below before their personal data is processed, or at the next practical opportunity:

- description of the personal data to be entered into the system;
- purposes for which they are being or will be processed, including processing for direct marketing, profiling, or historical, statistical, or scientific purpose;
- basis of processing, when processing is not based on the consent of the data subject;
- scope and method of the personal data processing;
- the recipients or classes of recipients to whom the personal data are or may be disclosed;
- methods utilised for automated access, if the same is allowed by the data subject, and the extent to which such access is authorised, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- the identity and contact details of the personal information controller and its representative;
- the period for which the information will be stored or retained; and
- the existence of their rights as data subjects.

Accordingly, the 'next practical opportunity' depends upon the surrounding circumstance of the case. However, the timing of the provision of information must always be within a reasonable period.

When a data subject objects or withholds consent, the controller must no longer process the personal data, unless:

- the personal data is needed pursuant to a subpoena;

- 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; or
- the information is being collected and processed as a result of a legal obligation.

Notably, in NPC Advisory Opinion No. 2017-042, the NPC opined that the consent contemplated by the Act is express consent by which the data subject voluntarily assents to the collection and processing of personal information through an overt act, such as signing or ticking a box, as the Act does not recognise implied or inferred consent resulting from the data subject's inaction or continued use or availment of services offered by a particular entity, except in specific circumstances where consent is not necessary in the first place.

Further, the NPC clarified in NPC Advisory Opinion No. 2017-017 that consent 'for any future legitimate use by a business' constitutes blanket authorisation that does not qualify as a specific and informed indication of will. In NPC Advisory 2021-01, the NPC advised that when a data subject objects or withholds consent, if there are allowable grounds for the controller to continue processing, said controller shall have the burden of determining the proving the appropriate lawful basis or compelling reason to continue such processing. Further, the controller must communicate and inform the data subject of said lawful basis to continue processing.

Specific cookie consent requirements and guidance

The NPC has not issued guidelines on the use of cookies and the collection of data subjects' consent for the same.

The NPC, however, discussed cookies briefly in the Advisory Opinion 47, where it opined that cookies, when combined with other pieces of information, may allow an individual to be distinguished from others, and may therefore be considered as personal information. As such, when the use of cookies involves the processing of a data subject's personal information, it is within the scope of the Act.

Furthermore, in the Advisory Opinion 63, the NPC opined on the matter of whether information about the use of cookies in pop-ups format is still required by the Act if it is already stated in the privacy policy. The NPC opined that the controller or processor has discretion as to whether additional means of informing the data subjects, such as through pop-ups in the website, would still be beneficial in complying with the Act and upholding data subjects' rights, particularly if the privacy policy is already adequate, accessible, and comprehensible. Accordingly, each controller and processor is in

the best position to determine the best mechanism to show their adherence to the principle of transparency given their unique circumstances. Thus, the use of pop-ups, while not required, may serve as an immediately accessible notice to data subjects.

As there are no specific requirements for acquiring consent for the use of cookies or similar technologies under the Act or pursuant to any NPC issuances, the general requirements for consent, as discussed above, apply.

There are likewise no guidelines on the further processing of personal information acquired from the use of cookies. The Act, however, provides that further processing of personal data collected from a party other than the data subject, such as the sharing of data acquired from the use of cookies, shall be allowed under any of the following conditions (Section 20 of the IRR):

- when it is expressly authorised by law, provided that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose, and proportionality;
- when, in the private sector, the data subject consents to data sharing and the following conditions are complied with:
    - consent for data sharing is acquired, even when the data is to be shared with an affiliate, mother company or similar relationships; and
    - when the data sharing is for commercial purposes, including direct marketing, it is covered by a data sharing agreement that establishes adequate safeguards for data privacy and security and upholds the rights of data subjects, such agreement potentially being subject to review by the NPC on its own initiative or upon a data subject's complaint.
- the data subject is provided with the following information prior to the collection or before data is shared:
    - the identity of the controllers or processors that will be given access to the personal data;
    - the purpose of data sharing;
    - the categories of personal data concerned;
    - the intended recipients or categories of recipients of the personal data;
    - the existence of the rights of data subjects, including the right to access and correction, and the right to object; and
    - any other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing; and
- any further processing of shared data shall adhere to the Act, the IRR and NPC issuances.

4. COOKIES & THIRD PARTIES

There are no specific rules on third-party cookies or cookies used by websites or platforms other than the website the user is visiting. However, as third-party cookies involve the processing of personal information, they are subject to the Act. Thus, points raised above on consent still apply.

5. COOKIE RETENTION

There are no specific rules on cookie retention periods or retention periods for similar technologies. The IRR, however, provides that the retention of personal data shall only be for as long as necessary:

- for the fulfilment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
- for the establishment, exercise, or defence of legal claims; or
- for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by the appropriate government agency.

Furthermore, personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined (Section 19 of the IRR).

6. OTHERS

Not applicable.

7. PENALTIES

There are no penalties specific for violations committed while using cookies to process users' personal information. The use of cookies without the consent of the data subject, however, may be liable for unauthorised processing (Section 52 of the IRR) or processing for unauthorised purposes of personal information and/or sensitive personal information (Section 55 of the IRR). These offences are punishable with imprisonment and a fine, which will depend on the type of personal data processed.

If the offender is a corporation, partnership, or any other juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime (Section 61 of the IRR).