Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2021-017[1]

8 June 2021

[redacted]

RE: INTELLECTUAL PROPERTY INVESTIGATION AND ENFORCEMENT AGENCIES' RIGHTS TO INQUIRY AND REQUEST FOR PERSONAL INFORMATION

Dear [redacted]

We write in response to your letter received by the National Privacy Commission (NPC) seeking an opinion on the metes and bounds of intellectual property (IP) investigation and enforcement agencies' rights to an unhampered inquiry and requests for basic data, which includes personal information, from online platforms as well as financial intermediaries, in connection with the agencies' investigation of suspected intellectual property rights (IPR) violations which are within the respective agencies' legal mandates.

We understand that the National Committee on Intellectual Property Rights (NCIPR) is considering having an online investigation protocol in relation to IP investigating agencies queries on suspected IPR violators.

Scope of the Data Privacy Act of 2012; criteria for lawful processing of personal data

The Data Privacy Act of 2012[2] (DPA) applies to the processing of personal information, sensitive personal information, and privileged information (collectively, personal data) of natural persons by the government and private entities and individuals, within and outside the Philippines.

The law likewise provides for the various criteria for processing personal data. Specifically in this scenario, Section 12 (e) of the DPA may be applicable. This provides for the processing of personal information necessary to fulfill functions of a public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

[1] Tags: law enforcement; investigation; mandate; due process; data sharing; data sharing agreement;
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], (2012).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph/ Email Add: info@privacy.gov.ph * Tel No. 8234-2228

In addition, for processing sensitive personal information and privileged information, Section 13 should likewise be considered. The said provision recognizes various lawful bases for processing applicable in this case, i.e., the processing is provided for by existing laws and regulations,[3] 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.[4]

Mandate of the NCIPR and member agencies; manner of requesting information; due process; general data privacy principles

In relation to the above, we understand that Executive Order (EO) No. 736[5] created the NCIPR. The said EO provides as one of the NCIPR's mandates is to intensify regular and effective enforcement against IPR violations, and to allocate sufficient resources to ensure effective prosecution of pirates and counterfeiters.[6]

The NCIPR is composed of the following agencies:

1. Department of Trade and Industry (DTI);
2. Intellectual Property Office of the Philippines (IPOPHIL);
3. Department of Justice (DOJ);
4. Department of the Interior and Local Government (DILG);
5. Bureau of Customs (BOC);
6. National Telecommunications Commission (NTC);
7. National Bureau of Investigation (NBI);
8. Philippine National Police (PNP);
9. Optical Media Board (OMB);
10. National Book Development Board (NBDB);
11. Food and Drug administration (FDA);
12. Office of the Special Envoy on Transnational Crime; and
13. Department of Information and Communications Technology (DICT).

In this regard, the processing of personal data by the NCIPR and its member agencies, pursuant to their respective mandates, is recognized under the DPA. The "metes and bounds" of these pertinent agencies' rights to inquire and request for information in relation to investigations and enforcement actions are essentially defined by their own respective constitutional and/or statutory mandates.

In this scenario, requests for information from online platforms and financial intermediaries may come in various forms, i.e., courts orders, subpoenas, officially issued orders, memoranda, letters, and other communication, among others, depending on several factors, such as the stage of the investigation or enforcement action as well as the powers of the particular member agency, i.e., some may have subpoena powers and while others do not.

[3] Data Privacy Act of 2012, § 13 (b).
[4] *Id.* § 13 (f).
[5] Office of the President, Institutionalizing Permanent Units To Promote, Protect And Enforce Intellectual Property Rights (IPR) In Different Law Enforcement And Other Agencies Under The Coordination Of The National Committee On Intellectual Property Rights (NCIPR), Executive Order No. 736 [E.O. No. 736] (June 21, 2008).
[6] E.O. No. 736, § 4.

While the NPC is not fully cognizant of all means and methods by which government agencies can validly request for information, essentially, the NPC simply requires that all agencies processing personal data, whether for law enforcement, investigative, regulatory, or some other public function, should strictly adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

Specifically, for the legitimate purpose principle, this presupposes that all due process requirements have been complied with in relation to any request for personal data. Likewise, for proportionality, the same requires that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

We emphasize that personal data processing activities of government agencies must not unreasonably infringe on the rights and freedoms of individuals guaranteed by the Constitution. Government agencies, as personal information controllers, are bound to uphold data subject rights provided for in the DPA.

Security of personal data; data sharing agreement

The NCIPR and its member agencies should consider the provisions of NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies, and NPC Circular No. 2020-03 on Data Sharing Agreements, as may be reasonable and appropriate with respect to the personal data processing activities of each agency in relation to its duties and responsibilities under EO No. 736 and related IPR laws, rules, and regulations.

We remind government agencies that the DPA is not meant to prevent them from processing personal data when necessary to fulfill their mandates. Rather, it aims to protect the right to information privacy while ensuring free flow of information. What the DPA does is to promote fair, secure, and lawful processing of such information.[7]

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

[7] See: National Privacy Commission, NPC Advisory Opinion No. 2019-046 (Dec. 17, 2019) citing NPC Advisory Opinion No. 2018-083 (Nov. 26, 2018).