Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2021-010[1]

22 March 2021

[redacted]

Re: PRIVATE DETECTIVE SERVICES

Dear [redacted]

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC). As a follow up to Advisory Opinion No. 2019-001,[2] you now seek further clarification on the applicability of the Data Privacy Act of 2012[3] (DPA) to the specific services and engagements of your company, Eyespy Detectives and Investigators Co. (Eyespy).

From your letter, we understand that Eyespy, a duly licensed private detective agency, offers the following services:

1. Surveillance Operations – includes monitoring the activities and movements of a data subject, following the data subject in his/her day-to-day activities, and taking pictures and/or videos. Eyespy does not record conversations but only take videos or pictures of activities or interactions of the data subject in public places.

2. Undercover Operations – mostly requested by business owners or proprietors, whereby Eyespy deploys undercover personnel in the premises or areas of operation to investigate or determine liability for anomalies or irregularities including theft and fraud, preparatory to possible administrative sanctions or criminal prosecution against responsible personnel. A licensed private detective is employed by the client-company to work in their premises and discreetly observe the activities of the client's employees during working hours.

3. Background Check – involves checking the information provided by the client on the data subject such as family, educational/professional background, and previous employment, among others, to determine whether the information provided by the data subject are truthful and accurate. Eyespy usually verifies the addresses, offices or establishment provided by the data subject and conducts discreet verification of the information provided.

1 Tags: Private detective services, background investigation, surveillance operations, undercover operations, lifestyle check, records check, right to privacy, lawful criteria for processing, data subject rights.
2 National Privacy Commission, NPC Advisory Opinion No. 2019-001 (Jan. 3, 2019).
3 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], Republic Act No. 10173 (2012).

4. Lifestyle Check – similar to surveillance investigation and background check except that the primary focus in the investigation is to determine whether the data subject is living within his or her means.

5. Records Check – involves checking and/or verifying with the records of private entities or government agencies any relevant information requested by the client in connection with the engagement.

Furthermore, you state that the services abovementioned are performed in connection with the following engagements:

1. Employers who request to investigate whether an employee is engaged in activities which violates employment stipulations such as non-competition clauses, exclusive employment (no moonlighting) clauses and other stipulations prohibiting employees from engaging in activities that are either in conflict or detrimental to the interest of the employer.

2. Insurance companies who ask to conduct Records Check and validate information/documents submitted by the insured or the latter's beneficiary. The Records Check usually requires validation of hospital, medical, police and/or funeral records. The insurance company would issue an authorization to Eyespy.

3. Creditors who plan to file collection suits against debtors but before doing so would ask Eyespy to perform Records Check to determine if the debtor has properties that can either be attached or used to satisfy any judgement issued for the case.

4. Foreign nationals or other individuals who request to conduct Background Check and Surveillance Operations on his/her Filipino partner in the Philippines before he/she continues to give support and/or proceed with the visa application to the foreign country.

5. A client who is either a principal, financier or business partner wants to check the general background and reputation of the subject person or company before deciding to enter into a business partnership.

6. A client who wants to check the activities of agents or employees in the Philippines to determine the latter's compliance with obligations under their contract.

7. A client whose rights to intellectual property is allegedly being infringed upon, requests Eyespy to obtain evidence of infringement and gather information about the infringer necessary for the application of a search warrant and/or prosecution.

8. A spouse who suspects marital infidelity of the other spouse, cohabiting with another person, or being engaged in any activity prejudicial to the marriage and the family. Eyespy is asked to conduct Surveillance Operations, including gathering of evidence to support cases for adultery, concubinage, annulment, legal separation, child custody, as may be applicable.

9. A client who is either the petitioner or the respondent in a guardianship case who wishes to interpose an objection to the appointment of another party as a guardian. Eyespy is asked to gather evidence which will be used in court to show that the adverse party is either disqualified or ill-suited to be appointed as guardian.

Eyespy posits it only accepts assignments that provide legal basis, i.e., protection or enforcement of the lawful rights or interest, and requires clients to accomplish a Service Request Form to provide a comprehensive background of the case and disclose the requested service. The potential client is notified beforehand that any information or report submitted

should be used exclusively for the purpose indicated in the Service Request Form and should not be disclosed or shared with any third party.

You now seek guidance and clarification on the legality and propriety of the services conducted by Eyespy vis-à-vis the engagements mentioned. From your letter, we gathered these specific inquiries:

1. Are the services conducted in connection with the engagements mentioned permissible and do not violate the DPA?
2. In the case of services performed for insurance companies: Is the authorization provided by the insurance company is already sufficient to authorize Eyespy to conduct Records Check?
3. In the case of Records Check for debt collection: Is Eyespy authorized under the DPA to gather information from pertinent government offices?
4. In the event that the data subject learns of the data gathering being conducted and demands that Eyespy cease and desist from data gathering and furnish the data subject a copy of all reports, information and data gathered, is Eyespy legally bound to comply with such demands? Is this appliable to any or all of the engagements?
5. In relation to Section 37 of the Implementing Rules and Regulations of the DPA (IRR), where the rights of the data subject "are also not applicable to the processing of personal data gathered for the purposes of investigations in relation to any criminal, administrative or tax liabilities of a data subject," is the same applicable to any or all of the abovementioned engagements?
6. In the case of Records Checks, how can Eyespy deal with data controllers who refuse access to records on the mistaken insistence that it is prohibited under the DPA?

Legality of processing personal data by private detective services; criteria for processing personal data

On the services provided by Eyespy, you propose that the same are all permissible data gathering activities pursuant to the provisions of the DPA, specifically Section 12 (b) - processing of personal information is necessary and is related to the fulfillment of a contract with the data subject and Section 13 (f) - 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.

While the above provisions of the DPA may be applicable to certain services in relation to some aforesaid engagements, i.e., relating to enforcement of existing contractual obligations for employment, insurance or loan-related matters, or in contemplation of or preparatory to, establishing, exercising or defending legal claims, it would be inaccurate to say that these provisions are the indeed the appropriate legal bases for Eyespy to carry out *all* of its services in relation to *all* the engagements earlier described.

Please note that the criteria for valid processing of personal and sensitive personal information (collectively, personal data) are enumerated in Sections 12 and 13 of the DPA, respectively. As discussed above, Section 12 (b) may be applicable in some instances where processing of personal information is related to or rooted on an existing contract between your client and the data subject, while Section 13 (f) may be applicable when processing sensitive personal information for legal claims or court proceedings.

With this, Eyespy should evaluate other possible lawful bases for processing, i.e., Section 12 (f) for processing personal information on legitimate interests pursued by the PIC 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, especially for those instances where there is no underlying contract involving the data subject and/or where Eyespy's client is not

considering any legal action or proceeding from such personal data processing activity.

In the determination of legitimate interest, the following must be considered:[4]

1. Purpose test – The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;
2. Necessity test – The processing of personal information must be necessary for the purpose of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test – The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PIC or third party, considering the likely impact of the processing on the data subjects.

Determination of DPA violation

As to the determination of whether there is a DPA violation in relation to the services provided by Eyespy, there can be no categorical statement to that effect based on the given information.

The Commission, where a complaint is filed or a *sua sponte* investigation is conducted, will have to take into consideration the circumstances of each situation and evidence submitted by the parties. Each case may be appreciated differently, depending on the manner of processing of personal data, whether there was adherence to the general data privacy principles, and data subject rights were upheld, among others.

We reiterate our position in *Advisory Opinion No. 2019-001*:

> "Given the foregoing, it is for Eyespy to determine whether its acts, such as records verification and background investigation, would: (a) constitute a violation of an individual's reasonable expectation of privacy, and (b) violate existing laws, including the DPA.
>
> Note that the DPA dictates that its provisions shall be liberally interpreted in a manner mindful of the rights and interests of the data subject. Thus, it is the burden of Eyespy to ensure that any processing of personal data is in accordance with the law."[5]

Conduct of Records Checks; authorization; general data privacy principles

In relation to Records Check services for insurance claims or cases, we wish to clarify that the authorization of the insurance company may just be one of the documents which may satisfy the requirements of the pertinent PIC to verify/validate the presented record or document.

Please note that the PIC being asked for the information will consider each request on a case-to-case basis, and must be satisfied that it is legitimate, within the lawful basis for processing under the DPA, and there is indeed an insurance claim or proceeding where the records validation is necessary for the purpose stated by the Eyespy.[6] The same may hold true for the records check for debt collection.

---

4 *See generally*, Data Privacy Act of 2012, § 12 (f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, *available at* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/.

5 National Privacy Commission, NPC Advisory Opinion No. 2019-001 (Jan. 3, 2019).

6 See: UK Information Commissioner's Office, When can I disclose information to a private investigator?, *available at* https://ico.org.uk/media/1556/disclosures_to_private_investigators.pdf (last accessed March 23, 2021).

In both cases, the affected data subject should have been informed at the outset, through the appropriate terms and conditions of the insurance contract, that verification of the information provided for insurance claims will be conducted when necessary, or in a loan agreement, whereby essential records will be verified/validated for purposes of debt collection.

Data subjects should therefore have an expectation that their personal data will be disclosed in relation to the aforementioned contractual obligations, subject to the general data privacy principles transparency, legitimate purpose, and proportionality.

Data subject rights in relation to private detective services; right to object; right to access; limitations

On the theoretical situation where the data subject learns of the personal data gathering conducted and demands Eyespy to cease and desist therefrom and furnish him or her a copy of all information gathered, Eyespy's compliance with such request will depend on the situation.

Note that while there may be a right to object to the processing of personal data, this applies in instances where processing is based on consent or legitimate interest. Hence, it is still possible to continue processing personal data where for example, the same is still 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.[7]

For further guidance, we refer to NPC Advisory No. 2021 – 01 on Data Subject Rights discussing the right to object, to wit:

> "SECTION 7. Right to Object. — x x x
>
> C. When a data subject objects, the PIC shall cease the processing of personal data and comply with the objection, unless the processing falls under any other allowable instances pursuant to in Sections 12 or 13, other than consent and legitimate interest.
>
> Should there be other grounds to continue processing the personal data, the PIC shall have the burden of determining and proving the appropriate lawful basis or compelling reason to continue such processing. The PIC shall communicate and inform the data subject of said lawful basis or compelling reason to continue processing."[8]

On the request to furnish a copy of the personal data collected, this may be anchored on the data subject right to access, and generally, may be granted by Eyespy. As an exception, this right may be limited when necessary for public interest, protection of other fundamental rights, or there exists a legitimate purpose justifying such limitation, which shall be proportional to the purpose of such limitation.[9]

Further, on the limitation provided in Section 37 of the IRR which you mentioned, the provision states in part:

> "Section 37. Limitation on Rights. The immediately preceding sections shall not be

7 Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34 (b) (2) (2016).
8 National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021 – 01] § 7 (C) (January 29, 2021).
9 *Id.* § 13 and 13 (D).

> applicable x x x. The said sections are also not applicable to the processing of personal data gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject. Any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research or investigation."

The nature of investigations in the above provision pertain to those conducted by government agencies based on their respective mandates. This does not contemplate investigations made by private parties, even when it is in relation to an alleged crime such as adultery or concubinage as described in your letter. We again refer to NPC Advisory No. 2021 – 01 for further guidance:

> "SECTION 13. Limitations. — x x x
>
> B. Investigations in relation to any criminal, administrative, or tax liabilities of a data subject: provided, that:
>
> 1. The investigation is being conducted by persons or entities duly authorized by law or regulation;
> 2. The investigation or any stage thereof relates to any criminal, administrative, or tax liabilities of a data subject as may be defined under existing laws and regulations; and
> 3. The limitation applies to the extent that complying with the requirements of upholding data subject rights would prevent, impair, or otherwise prejudice the investigation. x x x"

Refusal of PICs to grant access to records

As mentioned above, PICs would have to make their own evaluation of the legitimacy of the requests for access and disclosure to personal data on a case-to-case basis, and must be sufficiently convinced that indeed, the personal data is necessary for the declared purpose, and that the processing is fair, lawful, may have been reasonably expected by the data subject in case of existing contractual obligations or legal claims, and/or within the legitimate interests of the client which is balanced with the rights and freedoms of the data subject.

Eyespy may likewise communicate with the data protection officers of these PICs and clarify its lawful basis for requesting records, keeping in mind that these organizations and government agencies may have already established procedures on access to personal data which should be complied with.

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