Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-27

23 June 2017

[redacted]

Re: ANONYMIZED DATA FOR MARKETING ANALYTICS

Dear [redacted],

This pertains to your query received by the National Privacy Commission (NPC) on 12 May 2017, via AskPriva. You inquired if anonymized statistical data collected through a software for marketing analytics will fall within the scope of the Data Privacy Act (DPA) of 2012.

We understand that your company will collect data on demographics such as age, sex, gender, and location, for marketing analytics which would help your clients to market their products, and this data would not directly and certainly identify an individual.

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.[1] Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[2]

Information is anonymous when such information "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[3] Both Regulation (EU) 2016/679, which repeals the 1995 EU Directive upon which the DPA is based on, recognizes that "the principles of data protection should not apply to anonymous information."[4]

We note however the pertinent discussion in *Opinion 05/2014 on Anonymisation Techniques* of the Article 29 Data Protection Working Party of the European Commission, to wit:

> "xxx to anonymise any data, the data must be stripped of sufficient elements such that the data subject can no longer be identified. More precisely, the data must be processed in such a way that it can no longer be used to identify a natural person by

[1] R.A. 10173 (2012), §4
[2] Id., §3(g)
[3] Recital 26, Regulation (EU) 2016/679
[4] Regulation (EU) 2016/679 and DIRECTIVE 95/46/EC, Recital 26

> using "all the means likely reasonably to be used" by either the controller or a third party. An important factor is that the processing must be irreversible. xxx The focus is on the outcome: that data should be such as not to allow the data subject to be identified via "all" "likely" and "reasonable" means. Reference is made to codes of conduct as a tool to set out possible anonymisation mechanisms as well as retention in a form in which identification of the data subject is "no longer possible"."[5]

Further, the Opinion states that an effective anonymization solution prevents all parties (the personal information controller and any other person) from singling out an individual, to wit:

> "An effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset. Generally speaking, therefore, removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification, once again depending on the context and purposes of the processing for which the anonymised data are intended.
>
> xxx
>
> It must be clear that 'identification' not only means the possibility of retrieving a person's name and/or address, but also includes potential identifiability by singling out, linkability and inference. Furthermore, for data protection law to apply, it does not matter what the intentions are of the data controller or recipient. As long as the data are identifiable, data protection rules apply."[6]

The Opinion likewise provided an illustration on how a dataset would qualify as anonymous:

> "If an organisation collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties. But if the data controller would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as 'on Mondays on trajectory X there are 160% more passengers than on Tuesdays', that would qualify as anonymous data."[7]

From the foregoing discussions on scope of the law, definition of personal information, and what would constitute anonymous data, we believe that anonymized data, in its truest sense, is not considered as personal information and thus, falls outside of the ambit of the DPA.

However, for the proposed collection of data on demographics (age, sex, gender, and location) for marketing analytics, there is a need to further analyze and determine if this dataset is genuinely anonymized data as the original raw data containing identifiers for this dataset may still exist.

---

[5] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, §2.1 – Definition in the EU legal context

[6] Id., §2.2.2 – Potential identifiability of anonymized data

[7] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, §2.2.2 – Potential identifiability of anonymized data

Another factor to consider is the manner by which such data will be collected, and whether in the process, the company will have access to the database containing complete records, including personal data that has not yet been anonymized. If the company has access to the complete records, then the fact that the processing results in anonymized data, would not exempt the company from the coverage of the data privacy act.

Lastly, we wish to emphasize that if your company is processing personal data in some other manner and capacity, i.e. for human resource, outsourcing, etc., it is considered to be either a personal information controller or personal information processor, as the case may be, and thus, is required to comply with the provisions of the DPA, its Implementing Rules and Regulations (IRR) and related issuances of the NPC.

These other factors should be considered in evaluating whether the processing falls within the scope of the Data Privacy Act.

This advisory opinion is based on the limited information provided in the questions, and may vary based on additional information or when the facts are changed or elaborated.

For your reference. [8]

Very truly yours,

IVY D. PATDU
Officer-in-Charge
Deputy Privacy Commissioner for Policies

[8] This advisory opinion is based on the limited information provided in the questions, and may vary based on additional information or when the facts are changed or elaborated.