Date: 12 January 2021

Memorandum of Understanding

between:

The Information Commissioner

for

The United Kingdom of Great Britain & Northern Ireland

- and -

The National Privacy Commission

of

The Philippines

for Cooperation in the Regulation of Laws Protecting Personal Data

1. INTRODUCTION

1.1 This Memorandum of Understanding ("**MoU**") establishes a framework for cooperation between

(I) The Information Commissioner (the "**Commissioner**") and

(II) The National Privacy Commission (the "**NPC**"),

each a "**Participant**" and together the "**Participants**".

1.2 The Participants recognise the nature of the modern global economy, the increase in circulation and exchange of personal data across borders, the increasing complexity of information technologies, and the resulting need for increased cross-border enforcement cooperation.

1.3 The Participants acknowledge that they have similar functions and duties for the protection of personal information in their respective countries.

1.4 This MoU reaffirms the intent of the Participants to deepen their existing relations and to promote exchanges to assist each other in the enforcement of laws protecting personal information.

1.5 This MoU sets out the broad principles of collaboration between the Participants and the legal framework governing the sharing of relevant information and intelligence between them, excluding always the sharing of personal information.

1.6 The Participants confirm that nothing in this MoU should be interpreted as imposing a legal requirement on the participants to co-operate with each other. In particular, there is no requirement to co-operate in circumstances which would breach either Party's legal responsibilities, including:

(a) in the case of the Commissioner: the General Data Protection Regulation (the "**GDPR**") and other legislation listed in Paragraph 2.2; and

(b) in the case of the NPC: Republic Act No. 10173, otherwise known as The Data Privacy Act of 2012 ("**DPA 2012"**) and other legislation listed in Paragraph 3.2.

1.7 The MoU sets out the legal framework for information sharing, but it is for each Participant to determine for themselves that any proposed disclosure is compliant with the law applicable to them.

2. The role and function of the Information Commissioner

2.1 The Commissioner is a corporation sole appointed by Her Majesty the Queen under the Data Protection Act 2018 (the "**DPA**") to act as the UK's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

2.2 The Commissioner is empowered to take a range of regulatory action for breaches of the following legislation (as amended from time to time):

(a) Data Protection Act 2018 ("DPA");

(b) The General Data Protection Regulation ("GDPR");

(c) Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR");

(d) Freedom of Information Act 2000 ("FOIA");

(e) Environmental Information Regulations 2004 ("EIR");

(f) Environmental Protection Public Sector Information Regulations 2009 ("INSPIRE Regulations");

(g) Investigatory Powers Act 2016;

(h) Re-use of Public Sector Information Regulations 2015;

(i) Enterprise Act 2002;

(j) Security of Network and Information Systems Directive ("NIS Directive"); and

(k) Electronic Identification, Authentication and Trust Services Regulation ("eIDAS").

2.3 The Commissioner has a broad range of statutory duties, including monitoring and enforcement of data protection laws, and promotion of good practice and adherence to the data protection obligations by those who process personal data. These duties sit alongside those relating to the other enforcement regimes.

2.4 The Commissioner's regulatory and enforcement powers include:

(a) conducting assessments of compliance with the DPA, GDPR, PECR, eIDAS, the NIS Directive, FOIA and EIR;

(b) issuing information notices requiring individuals, controllers or processors to provide information in relation to an investigation;

(c) issuing enforcement notices, warnings, reprimands, practice recommendations and other orders requiring specific actions by an individual or organisation to resolve breaches (including potential breaches) of data protection legislation and other information rights obligations;

(d) administering fines by way of penalty notices in the circumstances set out in section 152 of the DPA;

(e) administering fixed penalties for failing to meet specific obligations (such as failing to pay the relevant fee to the Commissioner);

(f) issuing decision notices detailing the outcome of an investigation under FOIA or EIR;

(g) certifying contempt of court should an authority fail to comply with an information notice, decision notice or enforcement notice under FOIA or EIR; and

(h) prosecuting criminal offences before Courts.

2.5 Regulation 31 of PECR, as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, also provides the Commissioner with the power to serve enforcement notices and issue monetary penalty notices as above to organisations who breach PECR. This includes, but is not limited to, breaches in the form of unsolicited marketing which falls within the ambit of PECR, including automated telephone calls made without consent, live

telephone calls which have not been screened against the Telephone Preference Service, and unsolicited electronic messages (Regulations 19, 21 and 22 of PECR respectively).

3. The role and function of the National Privacy Commission

3.1 The Republic of the Philippines recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

3.2 The NPC is an independent body mandated to administer and implement the DPA 2012 and to monitor and ensure compliance of the Philippines with international standards set for data protection.

3.3 The Privacy Commissioner and the Deputy Privacy Commissioners of the NPC are appointed by the President of the Republic of the Philippines to lead the NPC in the performance of its mandate, duties and responsibilities, to safeguard the rights of the data subjects, ensure compliance of personal information controllers, personal information processors and other stakeholders to protect the fundamental human right to privacy, while ensuring free flow of information to promote innovation and growth.

3.4 The NPC has the following functions:

(a) ensure compliance of personal information controllers with the provisions of the DPA 2012;

(b) receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and in cases it deems appropriate, publicize such report;

(c) issue cease and desist orders, impose temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;

(d) compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;

(e) monitor compliance of other government agencies or instrumentalities on their security and technical measures and recommend necessary action in order to meet minimum standards for protection of personal information pursuant to the DPA 2012;

(f) coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;

(g) publish on a regular basis a guide to all laws relating to data protection;

(h) publish a compilation of agency system of records and notices, including index and other finding aids;

(i) recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified under Section 25 to 29 of the DPA 2012;

(j) review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers;

(k) provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;

(l) comment on the implication of data privacy of proposed national or local statues, regulations or procedures, issue advisory opinions and interpret the provisions of the DPA 2012 and other data privacy laws;

(m) propose legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary;

(n) ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection;

(o) negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

(p) assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and

(q) generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.

3.5 In furtherance of the mandate of the NPC, it likewise seeks to perform the following roles:

(a) be the authority in the Philippines on data privacy and protection, providing knowledge, know-how, and relevant technological guidance to its stakeholders;

(b) establish a regulatory environment that ensures accountability in the processing of personal data and promotes global standards for data privacy and protection;

(c) ensure cooperation between and among data privacy authorities and regulators to ensure effective implementation of privacy laws, share best practices and develop initiatives on data privacy and protection in the region and in the world;

(d) promote cross-border cooperation and regulatory collaboration; and

(e) build a culture of privacy, through people empowerment, that enables and upholds the right to privacy and supports free flow of information.

4. SCOPE OF CO-OPERATION

4.1 The Participants acknowledge that it is in their common interest to collaborate in accordance with this MoU, in order to:

(a) Ensure that the Participants are able to deliver the regulatory cooperation necessary to underpin their data-based economies and protect the fundamental rights of citizens of the United

Kingdom and the Philippines, respectively, in accordance with the applicable laws of the Participants' respective jurisdictions;

(b) Cooperate with respect to the enforcement of their respective applicable data protection and privacy laws, provided that it is not in contravention of national security and other relevant laws stated in sections 6 and 7.

(c) Keep each other informed of developments in their respective countries having a bearing on this MoU; provided that there is no law prohibiting the act; and

(d) Recognise parallel or joint investigations or enforcement actions by the Participants as priority issues for co-operation, subject to foreign relation laws of each Participant.

4.2 For this purpose, the Participants may jointly identify one or more areas or initiatives for cooperation. Such cooperation may include:

(a) sharing of experiences and exchange of best practices on data protection policies, education and training programmes;

(b) implementation of joint research projects;

(c) exchange of information (excluding personal data) involving potential or on-going investigations of organisations in the respective jurisdictions in relation to a contravention of personal data protection legislation;

(d) joint investigations into cross border personal data breaches or other security incidents involving organisations in both jurisdictions (excluding sharing of personal data);

(e) convening bilateral meetings annually or as mutually decided between the Participants; and

(f) any other areas of cooperation as mutually decided by the Participants.

4.3 This MoU does not impose on either the Commissioner or the NPC any obligation to co-operate with each other or to share any information. Where a Participant chooses to exercise its discretion to co-operate or to share information, it may limit or impose conditions on that request.

This includes where (i) it is outside the scope of this MoU, or (ii) compliance with the request would breach the Participant's legal responsibilities.

4.4 Participants agree that the sharing of information will not imply any transfer of ownership or rights in connection with the shared information.

5. NO SHARING OF PERSONAL DATA

5.1 The Participants do not intend that this MoU shall cover any sharing of personal data by the Participants. For the purpose of this MOU, personal data will be given the meaning defined in the relevant Participant's domestic law.

5.2 If the Participants wish to share personal data, for example in relation to any cross border personal data breaches or other security incidents involving organisations in both jurisdictions, each Participant shall consider compliance with its own applicable data protection laws, which may require the Participants to enter into a written agreement or arrangement regarding the sharing of such personal data. Provisions under Paragraphs 6 and 7 shall be taken into consideration prior to any such sharing of personal data.

6. INFORMATION SHARED BY THE COMMISSIONER

6.1 Section 132(1) of the DPA 2018 states that the Commissioner can only share certain information if she has lawful authority to do so, where that information has been obtained, or provided to, the Commissioner in the course of, or for the purposes of, discharging the Commissioner's functions, relates to an identifiable individual or business, and is not otherwise available to the public from other sources.

6.2 Section 132(2) of the DPA 2018 sets out the circumstances in which the Commissioner will have the lawful authority to share that information. Of particular relevance when the Commissioner is sharing information with the NPC are the following circumstances, where:

(a) The sharing is necessary for the purpose of discharging the Commissioner's functions (section 132(2)(c));and

(b) The sharing is necessary in the public interest, taking into account the rights, freedoms and legitimate interests of any person (section 132(2)(f)).

6.3 Before the Commissioner shares such information with the NPC, the Commissioner may identify the function of the NPC with which that information may assist, and assess whether that function of the NPC could reasonably be achieved without access to the particular information in question.

6.4 The Commissioner may choose to share certain information with the NPC only if the NPC agrees to certain limitations on how it may use that information.

7. INFORMATION SHARED BY THE NPC

7.1 Section 8 of the DPA 2012 states that the NPC shall ensure at all times the confidentiality of any personal information that comes to its knowledge and possession.

7.2 Before sharing such information with the Commission, the NPC shall identify the function of the Commission with which that information may assist, and assess whether that function of the Commission could reasonably be achieved without access to the particular information in question, provided further, that the following laws shall be taken into consideration:

(i) NPC shall adhere to Executive Order No. 246 creating the National Intelligence Coordinating Agency (NICA). NICA is mandated to be the focal point for the direction, coordination and integration of government activities involving national intelligence, and the preparation of intelligence estimates of local and foreign situations for the formulation of national policies by the President.

(ii) NPC shall adhere to Republic Act No. 7157 otherwise known as the "Philippine Foreign Service Act of 1991", mandating

the Department of Foreign Affairs to implement the three (3) pillars of the Philippine Foreign Policy:

- Preservation and enhancement of national security
- Promotion and attainment of economic security
- Protection of the rights and promotion of the welfare and interest of Filipinos overseas.

8. SECURITY AND DATA BREACH REPORTING

8.1 Appropriate security measures shall be agreed upon to protect information transfers in accordance with the sensitivity of the information and any classification that is applied by the sender.

8.2 Where confidential material is shared between the Participants it will be marked with the appropriate security classification.

8.3 Where one Participant has received information from the other, it will consult with the other Participant before passing the information to a third party or using the information in an enforcement proceeding or court case. Paragraphs 6 and 7 of this MOU shall be taken into consideration prior to any such onward sharing of information.

8.4 Where confidential material obtained from, or shared by, the originating Participant is wrongfully disclosed or used by the receiving Participant, the receiving Participant will bring this to the attention of the originating Participant without delay.

9. REVIEW OF THE MoU

9.1 The Commissioner and the NPC will monitor the operation of this MoU and review it biennially, or sooner if either Participant so requests.

9.2 Any issues arising in relation to this MoU will be notified to the designated point of contact for each Participant.

9.3 This MoU may only be amended by the Participants in writing and signed by each Participant.

10. NON-BINDING EFFECT OF THIS MoU AND DISPUTE SETTLEMENT

10.1 This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the Commissioner or the NPC.

10.2 The Participants will settle any disputes or disagreement relating to or arising from this MoU amicably through consultations and negotiations in good faith without reference to any international court, tribunal or other forum.

11. DESIGNATED CONTACT POINTS

11.1 The following persons shall be the designated contact points for the Participants for matters under this MoU:

Information Commissioner's Office	**National Privacy Commission**
Name: Adam Stevens Designation: Head of Intelligence	Name: Ivy Grace T. Villasoto Designation: OIC - Director IV, Privacy Policy Office

11.2 The above individuals will maintain an open dialogue between each other in order to ensure that the MoU remains effective and fit for purpose. They will also seek to identify any difficulties in the working relationship, and proactively seek to minimise the same.

11.3 Each Participant may change its designated contact point for the purposes of this MoU upon notice in writing to the other Participant.

12. EFFECTIVITY

12.1 This MoU shall come into effect on the date of signature of both Parties.

Signatories:

Elizabeth Denham **Information Commissioner**	**Raymund Enriquez Liboro** **Privacy Commissioner**
[redacted] Date: 12 January 2021	[redacted] Date: 12 January 2021