

**MEMORANDUM OF UNDERSTANDING**  
**BETWEEN**  
**THE PRIVACY COMMISSIONER FOR PERSONAL DATA OF**  
**HONG KONG, CHINA**  
**AND**  
**THE INFORMATION COMMISSIONER FOR THE UNITED KINGDOM**  
**FOR COOPERATION IN**  
**PROTECTING PERSONAL DATA**

The Privacy Commissioner for Personal Data of Hong Kong, China (hereinafter referred to as “PCPD”) and the Information Commissioner for the United Kingdom (hereinafter referred to as “**the Commissioner**”), hereinafter referred to individually as the “**Participant**” and collectively as the “**Participants**”,

**Reaffirming** their intent to deepen their existing relations and to promote exchanges in personal data protection;

**Recognising** the need to foster closer collaboration and cooperation in personal data protection;

**Confirming** that nothing in this Memorandum of Understanding (hereinafter referred to as “**MOU**”) should be interpreted as imposing a requirement on the Commissioner to cooperate with PCPD in circumstances where doing so would breach the Commissioner’s legal responsibilities, including under the legislation listed in Paragraph 3 (Role and function of the Commissioner);

**Confirming** that nothing in this MOU should be interpreted as imposing a requirement on the PCPD to cooperate with the Commissioner in circumstances where doing so would breach its statutory obligations and powers under the Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong Special Administrative Region) (“**PDPO**”); and/or other legal requirements under the Laws of Hong Kong Special Administrative Region

**HAVE REACHED** the following understandings on a framework for cooperation which sets out non-binding broad principles of collaboration and the legal framework governing the sharing of relevant information between the Participants:

**PARAGRAPH 1**

**SCOPE OF COLLABORATION**

1) The Participants will collaborate in personal data protection in accordance with this MoU 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 Hong Kong Special Administrative Region of People’s Republic of China respectively, in accordance with the Participants’ respective applicable laws;

(b) Cooperate with respect to the enforcement of their respective applicable data protection and privacy laws;

(c) Keep each other informed of developments in their respective economies having a bearing on this MOU; and

(d) Recognise parallel or joint investigations or enforcement actions by the Participants as priority issues for co-operation.

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) co-operation in providing regulatory guidance in both jurisdictions to support innovation in technology or business models, in the form of cross-jurisdiction regulatory sandboxes or other similar mechanisms, with the Commissioner providing advice on United Kingdom information law and the PCPD providing advice on Hong Kong data protection law;

(c) implementation of joint research projects;

(d) exchange of information and research collaborations regarding the development and implementation of artificial intelligence governance framework and ethics;

(e) exchange of information (excluding personal data) involving potential or on-going enquiries of organisations in the respective economies on areas of personal data protection;

(f) joint investigations into cross border personal data incidents involving organisations in both jurisdictions (excluding sharing of personal data);

(g) convening bilateral exchange and training annually or as mutually decided between the data protection authorities of the Participants; and

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

## **PARAGRAPH 2**

### **SPECIFIC AGREEMENTS OR ARRANGEMENTS**

Each Participant may, within the limits of its respective laws and regulations and respective competence, enter into separate written agreements or arrangements with the other Participant, for the execution of projects or activities within the scope of this MOU.

## **PARAGRAPH 3**

### **ROLE AND FUNCTION OF THE COMMISSIONER**

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

2) The Commissioner is empowered to take a range of regulatory action for breaches of the following legislation (as may be amended, including as a consequence of the United Kingdom's withdrawal from the European Union), hereinafter referred to by their acronyms as indicated below:

- (a) DPA;
- (b) 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”).

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 outlined in paragraph 3(4) below.

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 the Courts.

5) Regulation 31 of PECR, 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).

#### **PARAGRAPH 4**

##### **ROLES AND FUNCTIONS OF PCPD**

1) The PCPD is a corporation sole established under the PDPO and an independent statutory body to oversee the compliance of the PDPO which is enacted to protect the privacy of individuals in relation to personal data.

2) The PCPD has a broad range of statutory functions, including :

(a) monitor and supervise compliance with the provisions of the PDPO;

(b) promote and assist bodies representing data users to prepare codes of practice for guidance in complying with the provisions of the PDPO, in particular the data protection principles;

(c) promote awareness and understanding of, and compliance with, the provisions of the PDPO, in particular the data protection principles;

(d) examine any proposed legislation (including subsidiary legislation) that the PCPD considers may affect the privacy of individuals in relation to personal data and report the results of the examination to the person proposing the legislation;

(e) carry out inspections, including inspections of any personal data systems used by data users which are departments of the Government of Hong Kong Special Administrative Region or statutory corporations;

(f) for the better performance of his other functions, undertake research into, and monitor developments in, the processing of data and information technology in order to take account of any likely adverse effects such developments may have on the privacy of individuals in relation to personal data;

(g) liaise and co-operate with any person in any place outside Hong Kong—(i) performing in that place any functions which, in the opinion of the PCPD, are similar (whether in whole or in part) to any of the PCPD's functions under the PDPO; and (ii) in respect of matters of mutual interest concerning the privacy of individuals in relation to personal data; and

(h) perform such other functions as are imposed on him under the PDPO or any other enactment.

3) The PCPD's regulatory and enforcement powers include, among others:

a) carry out inspection of personal data systems;

b) carry out investigation upon receipt of a complaint or having reasonable belief that the relevant act or practice contravenes the PDPO;

- c) give consent to a matching procedure request and specify conditions for a matching procedure;
- d) enter premises for inspection or investigation;
- e) conduct proceedings for purposes of investigation;
- f) summon any person to give evidence, examine any person and require any person to give evidence for purposes of investigation;
- g) publish a report in relation to an inspection and investigation;
- h) serve enforcement notices, which specify, inter alia, (i) the requirement which, in the opinion of the PCPD, is being or has been contravened; (ii) the act or omission that constitutes the contravention; (iii) the steps that the data user must take (including ceasing any act or practice) to remedy and, if appropriate, prevent any recurrence of the contravention; (iv) the date on or before which the steps must be taken; and
- i) assist aggrieved person for instituting proceedings for compensation under section 66 (e.g. obtaining information, giving advice, arranging for legal assistance).

#### **PARAGRAPH 5**

##### **NO SHARING OF PERSONAL DATA**

- 1) The Participants do not intend that this MOU shall cover any sharing of personal data by the Participants.
- 2) If the Participants wish to share personal data, for example in relation to any cross border personal data 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 separate written agreement or arrangement regarding each occasion of sharing of such personal data.

#### **PARAGRAPH 6**

##### **COSTS, EXPENSES AND RESOURCES**

Without prejudice to any separate written agreement or arrangement under Paragraph 2 or unless otherwise mutually decided upon in writing by the Participants, each Participant will bear its own costs and expenses in implementing this MOU.

#### **PARAGRAPH 7**

##### **CONFIDENTIAL INFORMATION SHARED BY THE COMMISSIONER**

- 1) Section 132(1) of the DPA 2018 states that the Commissioner can only share confidential information with others if there is lawful authority to do so. In this context, the information will be considered confidential if it 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. Section 132(2) of the DPA 2018 sets out the circumstances in which the Commissioner will have the lawful authority to share that confidential information with the PCPD. In particular, it will be lawful in circumstances where:

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

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

2) The Commissioner will therefore be permitted to share confidential information with the PCPD in circumstances where the Commissioner has determined that it is reasonably necessary to do so in furtherance of the Commissioner's role and functions. In doing so, the Commissioner will identify the function of the PCPD with which that information may assist, and assess whether that function of the PCPD could reasonably be achieved without access to the particular information in question.

3) The Commissioner may exercise the discretion to refuse, limit or impose conditions on a request for cooperation with the PCPD where (i) it is outside the scope of this MOU, or (ii) compliance with the request would breach the Commissioner's legal responsibilities, including under the GDPR.

## **PARAGRAPH 8**

### **CONFIDENTIAL INFORMATION SHARED BY PCPD**

1) Subject to the subparagraphs below, section 46(1) of the PDPO stipulates that the PCPD and every prescribed officer shall maintain secrecy in respect of all matters that come to their actual knowledge in the performance of their functions and the exercise of their powers during conducting inspections, handling complaints and carrying out investigations.

2) Sections 46(7) & (8) set out the circumstances in which the PCPD may share the matters with the Commissioner.

3) Pursuant to section 46(7) of the PDPO, the PCPD may disclose matters to a privacy regulatory authority outside of Hong Kong, for the purpose of enabling or assisting that authority to perform a relevant function of that authority, if -

(a) that authority has undertaken to be bound by the secrecy requirements imposed by the PCPD; and

(b) in the opinion of the PCPD, there is in force in that place any law which is substantially similar to, or serves the same purposes as the PDPO.

4) Section 46(8) of the PDPO further provides that the Commissioner may, for the proper performance of the PCPD's functions or the proper exercise of the PCPD's powers under the PDPO, disclose matters to a privacy regulatory authority outside of Hong Kong that performs a relevant function, if--

(a) that authority has undertaken to be bound by the secrecy requirements imposed by the PCPD; and

(b) any of the following conditions is satisfied:

(i) in the opinion of the PCPD, there is in force in that place any law which is substantially similar to, or serves the same purposes as, the PDPO;

(ii) the data subject to whom the matter relates has consented in writing to the disclosure;

(iii) the PCPD has reasonable grounds for believing that, in all the circumstances of the case, the disclosure is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that disclosure; and if it was practicable to obtain such consent, the data subject would give it;

(iv) the personal data to which the matters relate is exempt from the provisions of data protection principle 3 because of an exemption under Part 8 of the PDPO; or

(v) the PCPD has taken all reasonable precautions and exercised all due diligence to ensure that the personal data to which the matters relate will not, in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the PDPO.

5) “Relevant function” of an authority outside of Hong Kong under subparagraphs (3) & (4) above means a function relating to investigation into a suspected contravention, and enforcement, of legal or regulatory requirements in that place concerning the protection of privacy of individuals in relation to personal data.

6) The PCPD may therefore share confidential information with the Commissioner for the Commissioner’s performance of her relevant function if the conditions under section 46(7) or (8), where applicable, are satisfied. The sharing of confidential information will be subject to the Participants’ respective statutory requirements and obligations under a separate agreement and/or secrecy undertaking to be entered into regarding such occasion of sharing confidential information.

## **PARAGRAPH 9**

### **CONFIDENTIALITY AND DATA BREACH REPORTING**

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

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

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.

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

## **PARAGRAPH 10**

### **REVIEW**

1) The Commissioner and the PCPD will monitor the operation of this MOU and review it annually, or sooner if either Participant so chooses.

2) Any issues arising in relation to this MOU will be notified to the point of contact for each Participant.

**PARAGRAPH 11**

**AMENDMENTS**

Either Participant may make a request in writing for a revision or amendment of any provision of this MOU. Any revision or amendment which has been mutually decided upon in writing by the Participants will come into effect on such date as may be mutually decided upon by the Participants.

**PARAGRAPH 12**

**ENTRY INTO EFFECT, DURATION AND TERMINATION**

1) This MOU will take effect on the date of signature and will remain effective for a period of twelve (12) months. The term of this MOU may be extended by written consent of the Participants for such period or periods as the Participants may mutually decide upon.

2) Notwithstanding sub-paragraph (1) under this Paragraph, either Participant may terminate this MOU by giving six (6) months' written notice to the other Participant.

3) The termination of this MOU will not affect the validity, duration, implementation and completion of any project or activity undertaken or decided upon under this MOU prior to the date of termination unless the Participants otherwise mutually decide in writing.

**PARAGRAPH 13**

**DESIGNATED CONTACT POINTS**

1) The following shall be the designated contact points for the Participants for matters under this MOU:

|  |   |
|--|---|
| PCPD   | Information Commissioner's Office                       |
| Name: Ivan Chan<br>Designation: Head of Communications and Education | Name: Adam Stevens<br>Designation: Head of Intelligence |

2) The responsible officers of the Participants 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.

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

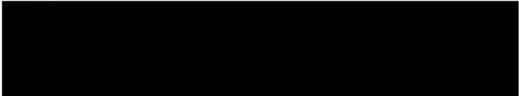
**PARAGRAPH 14**

**NON-BINDING EFFECT OF THIS MOU AND DISPUTE SETTLEMENT**

1) Nothing in this MOU is to be construed as establishing or implying a partnership, joint venture, agency or other legal relationship between the Participants. Nothing in this MOU creates or is intended to create any legally enforceable rights or binding obligations on either Participant.

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.

Signed in the English language on the 29 July 2020.

|   |  |
|---|--|
| The Privacy Commissioner for Personal Data<br>Hong Kong, China  | For the Information Commissioner of the<br>United Kingdom  |
| Signature<br><br>Name: Stephen Kai-yi Wong<br>Title: Privacy Commissioner for Personal Data,<br>Hong Kong, China | Signature<br><br>Name: Elizabeth Denham<br>Title: Information Commissioner |