Date: 5 July 2022

Memorandum of Understanding

between

the Information Commissioner

for

the United Kingdom of Great Britain and Northern Ireland

- and -

the Personal Information Protection Commission of the Republic of Korea

on Cooperation in the Regulation of Laws Protecting Personal Data

Introduction

The Information Commissioner for the United Kingdom of Great Britain and Northern Ireland (the "Commissioner") and the Personal Information Protection Commission of the Republic of Korea (the "PIPC") (hereafter jointly referred to as the "Participants");

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

Acknowledging that they have similar functions and duties for the protection of personal information in their respective countries;

Intending to deepen their existing relations and to promote exchanges to assist each other in the enforcement of laws protecting personal information;

Desiring to set out the broad principles of collaboration between the Participants and the framework governing the sharing of relevant information and intelligence, excluding the sharing of personal information;

Have reached the following understanding:

1. General Provisions

1.1 The Participants confirm that nothing in this Memorandum of Understanding ("MoU") should be interpreted as imposing a requirement on the Participants to cooperate with each other. In particular, there is no requirement to cooperate in circumstances which would breach their legal responsibilities, including:

(a) in the case of the Commissioner: the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) ("UK GDPR"); and

(b) in the case of the PIPC: the Personal Information Protection Act ("PIPA").

1.2 This MoU sets out the framework for information sharing, but it is for each Participant to determine for itself whether any proposed disclosure is compliant with the law applicable to it.

1.3 This MoU will be implemented subject to the availability of appropriated funds and personnel of the Participants.

2. The role and function of the Commissioner

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

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

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

(b) UK 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 the monitoring and enforcement of data protection laws, and the promotion of good practices 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, UK GDPR, PECR, eIDAS, 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 the PECR. This includes, but is not limited to, breaches in the form of unsolicited marketing which falls within the ambit of the 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 the PECR respectively).

3. The Role and Function of the PIPC

3.1 The PIPC was established under the Personal Information Protection Act and the Government Organization Act of the Republic of Korea. Its mission is to protect the freedom and rights of individuals and embody the dignity and values of individuals by prescribing the matters required for personal information processing and protection.

3.2 The PIPC may take regulatory actions for breaches of the relevant legislation including the following (as amended from time to time):

(a) Personal Information Protection Act ("PIPA");

(b) Credit Information Use and Protection Act ("Credit Information Act");

(c) Standard Guidelines on Personal Information Protection;

(d) Standards for Measures to Ensure the Security of Personal Information;

(e) Notification of Linkage and Release of Pseudonymized Data by Public Institutions;

(f) Notification of Linkage and Release of Pseudonymized Data, Etc.;

(g) Notification of Means to Process Personal Information; and

3.3 Standards for Technical and Organizational Measures to Protect Personal Information. The PIPC assumes a broad scope of legal obligations, including to supervise the compliance with the relevant laws and enforce such laws and to urge personal information controllers to comply with such laws.

3.4 The functions of the PIPC under Article 7-8 of the PIPA include:

(a) matters concerning the improvement of laws relating to personal information protection;

(b) matters concerning the establishment and implementation of policies, systems and/or plans relating to personal information protection;

(c) matters concerning investigation into infringement of the rights of data subjects and subsequent dispositions;

(d) handling of complaints and remedial procedures relating to personal information processing and mediation of disputes over personal information;

(e) exchange and cooperation with international organisations and overseas data protection authorities for the purpose of protecting personal information; and

(f) matters concerning investigations into and studies on, education on and the promotion of laws, policies, systems and status relating to personal information protection.

4. SCOPE OF COOPERATION

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 and residents of the United Kingdom and the Republic of Korea 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;

(c) keep each other informed of developments in their respective countries having a bearing on this MoU; and

(d) recognise parallel or joint investigations or enforcement actions by the Participants as priority issues for cooperation.

4.2 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 enforcement, personal data protection policies, education and training programmes;

(b) implementation of joint research projects;

(c) cooperation on regulatory and policy issues in relation to the development of new technology;

(d) exchange of information (excluding personal data) involving potential or on-going investigations of organisations in their respective jurisdictions in relation to a contravention of laws related to personal data protection;

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

(f) convening bilateral meetings annually or as mutually decided by the Participants;

(g) regular personnel exchange; and

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

4.3 This MoU does not impose any obligation on the Participants to cooperate with each other or to share any information. Where a Participant chooses to exercise its discretion to cooperate 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.

5. NO SHARING OF PERSONAL DATA

5.1 This MoU is not intended to cover any sharing of personal data by the Participants.

5.2 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 will consider compliance with its own applicable data protection laws, which may require the Participants to enter into a written arrangement regarding the sharing of such 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 the Commissioner 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 PIPC 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 PIPC, the Commissioner may identify the function of the PIPC with which that information may assist, and assess whether that function of the PIPC could reasonably be achieved without access to the particular information in question.

6.4 The Commissioner may choose to share certain information with the PIPC, provided that the PIPC consents to certain limitations on how it may use that information.

7. INFORMATION SHARED BY THE PIPC

7.1 In the event that the PIPC becomes aware of any violation or suspected violation of Article 63 (Request for Materials and Inspections) of the PIPA, it may request the relevant personal information controllers to submit materials such as articles and documents. However, the PIPC may not disclose documents and materials submitted or collected under Paragraph 8 of Article 63 to third parties or to the general public, unless otherwise prescribed in the PIPA.

7.2 No person who performs or has performed specific duties under the PIPA will divulge any confidential information acquired in the course of performing his or her duties to any other person or use such information for any purpose other than for his or her duties. The foregoing provision will not apply where divergent provisions exist in other Acts.

7.3 Prior to sharing information with the Commissioner, the PIPC may ask whether the information in question needs to be shared and assess whether the information may contribute to serving the public interest of the citizens and residents of the two countries.

7.4 When sharing information with the Commissioner, the PIPC may impose a restriction on the disclosure of any information related to the

Republic of Korea to third parties or outside organisations, and such information may only be shared where the Commissioner has consented to such a restriction.

8. SECURITY AND DATA BREACH REPORTING

8.1 Appropriate security measures will be jointly decided upon to protect information transfers in accordance with the sensitivity of the information and any classification that is applied by the originating Participant.

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.

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 AND AMENDMENT

9.1 The Participants 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 with the mutual written consent of the Participants.

10. NON-BINDING EFFECT 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 Participant.

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 will be the designated contact points for the Participants for matters under this MoU:

Information Commissioner's Office	**Personal Information Protection Commission**
Name: Rory Munro Designation: Head of International Regulatory Cooperation	Name: Yunah Kang Designation: Assistant Director, International Cooperation

11.2 The above contact points will maintain an open dialogue in order to ensure that this MoU remains effective and fit for its 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. ENTRY INTO EFFECT AND TERMINATION

This MoU will come into effect upon its signature by the Participants and remain in effect unless terminated by either Participant upon three months' written notice to the other Participant.

SIGNED in duplicate in the English language.

For the Information Commissioner for the United Kingdom of Great Britain and Northern Ireland

[redacted]

Name: [redacted]

Title:

Place:

Date:

For the Personal Information Protection Commission of the Republic of Korea

[redacted]

Name: [redacted]

Title:

Place:

Date: