Date: Wednesday, 12 May 2021

Memorandum of Understanding

between:

The Information Commissioner

for

The United Kingdom of Great Britain & Northern Ireland

- and -

The Office of the Privacy Commissioner

for

New Zealand

for Cooperation in the Enforcement 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 "**Information Commissioner**") and

(II) The Office of the Privacy Commissioner (the "**Privacy Commissioner**"),

together referred to as 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 requirement on the participants to co-operate with each other. In particular, there is no requirement to co-operate in circumstances which would breach their legal responsibilities, including:

(a) in the case of the Information Commissioner: the General Data Protection Regulation (the "**GDPR**"); and

(b) in the case of the Privacy Commissioner: the Privacy Act 2020 (the "**Privacy Act**").

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. ROLE AND FUNCTIONS OF THE INFORMATION COMMISSIONER

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

(a) The DPA;

(b) The GDPR, with the Participants acknowledging that references to GDPR should, where the context allows, be interpreted as meaning the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of the European Union (Withdrawal) Act 2018;

(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 Information 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 Information 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 Information 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 Information 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 fall 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. ROLE AND FUNCTIONS OF THE PRIVACY COMMISSIONER

3.1 The Privacy Commissioner is a corporation sole and independent crown entity appointed by the Minister of Justice under the Privacy Act. The role of the Privacy Commissioner is to lead the Office of the Privacy Commissioner as New Zealand's independent privacy and data protection regulator under the Privacy Act which governs how public and private sector agencies collect, use, disclose, store and give access to personal information, as well as codes of practice issued under the Privacy Act.

3.2 The Privacy Commissioner has extensive functions under the Privacy Act concerned with personal privacy and the general protection of individual privacy. These include:

(a) promoting, by education and publicity, an understanding and acceptance of the information privacy;
(b) making public statements on matters affecting individual privacy;
(c) receiving and investigating complaints about breaches of individual privacy;
(d) monitoring and examining the impact that technology has upon privacy;
(e) issuing codes of practice that modify the application of the privacy principles in relation to a particular type of information, agency, activity or industry;
(f) examining new legislation for its possible impact on individual privacy;
(g) monitoring information matching programmes between government departments;
(h) inquiring into any matter where it appears that individual privacy may be affected;

(i) assisting the responsible Minister with making regulations in relation to disclosure of personal information outside of New Zealand; and
(j) providing oversight to information sharing agreements.

3.3 The Privacy Commissioner also has oversight functions under other enactments relating to the provision of specialist insight on privacy matters, or in a safeguard and oversight role. These include:
(a) Health Act 1956 s22F;
(b) Family Violence Act 2018, ss 245 – 247 and the Family Violence Regulations 2019, reg 20;
(c) Social Security Act 2018, schedule 6, cls 8, 10 – 12;
(d) Passports Act 1992, s 36;
(e) Customs and Excise Act 2018, s 318;
(f) Official Information Act 1982, s 29B;
(g) Local Government Official Information and Meetings Act 1987, s 29A;
(h) Health and Disability Commissioner Act 1994, ss 23 and 36;
(i) Anti-Money Laundering and Countering Financing of Terrorism Act 2009, s 146;
(j) Ombudsmen Act 1975, s 17A;
(k) Intelligence and Security Act 2017, s 161;
(l) Corrections Act 2004, s 182D;
(m) Social Security Act 2018, schedule 6, cls 6 and 7;
(n) Education and Training Act 2020, schedule 9, cl 9; and
(o) Immigration Act 2009, s 32.

3.4 The Privacy Commissioner's regulatory and enforcement powers include to:
(a) issue a statutory demand notice requiring any person who in the Privacy Commissioner's opinion is able to give information relevant to an investigation or inquiry to furnish information or produce documents or things in their possession as a are relevant to the subject matter of the investigation or inquiry;
(b) summon and examine under oath any person who the Privacy Commissioner considers is able to give information relevant to an investigation;
(c) prosecute an offence under the Privacy Act;
(d) issue a compliance advice notice where the Privacy Commissioner has concerns about the conduct or practices of an agency;

(e) issue a compliance notice if the Privacy Commissioner considers that a breach of a privacy principle, code of practice, or interference with an individual's privacy has occurred;
(f) issue an access direction to an agency which requires that agency to provide an individual access to their personal information in any manner that the Privacy Commissioner considers appropriate (if an attempt to settle a complaint about a breach or interference with the privacy of an individual is unsuccessful);
(g) create and issue a code of practice that modifies the application of the information privacy principles as set out in the Privacy Act in relation to a particular type of information, agency, activity or industry;
(h) inquire into any matter where it appears that individual privacy may infringed; and
(i) issue a public statement where the Privacy Commissioner considers appropriate to comment on a subject matter which relates to the Privacy Act.

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 New Zealand 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 co-operation.

4.2 For the purposes of clause 4.1, 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) co-operation in any specific projects of interest;

(d) 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;

(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 between the Participants; and

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

4.3 This MoU does not impose on either the Information Commissioner or the Privacy Commissioner 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, that Participant may limit or impose conditions on that request. This includes circumstances where:

(a) the subject matter of the request is outside the scope of this MoU; or

(b) compliance with the request would breach a Participant's legal responsibilities.

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.

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 comply 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.

6. INFORMATION SHARED BY THE INFORMATION COMMISSIONER

6.1 Section 132(1) of the DPA 2018 states that the Information Commissioner can only share certain information if they have lawful authority to do so, where that information has been obtained, or provided to, the Information Commissioner in the course of, or for the purposes of, discharging the Information 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 Information Commissioner will have the lawful authority to share that information. Of particular relevance when the Information Commissioner is sharing information with the Privacy Commissioner are the following circumstances, where:

(a) The sharing is necessary for the purpose of discharging the Information 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 Information Commissioner shares the information referred to in clause 6.1 with the Privacy Commissioner, the Information Commissioner may identify the function of the Privacy Commissioner with which that information may assist and assess whether that function of the Privacy Commissioner could reasonably be achieved without access to the particular information in question.

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

7. INFORMATION SHARED BY THE PRIVACY COMMISSIONER

7.1 Section 207 of the Privacy Act allows the Privacy Commissioner to provide an overseas privacy enforcement authority with any information that the Privacy Commissioner holds in relation to the performance or exercise of their functions, duties, or powers at law, and considers this may:

(a) assist the authority in the performance or exercise of the authority's functions, duties, or powers under or in relation to any enactment; or

(b) enable the authority to reciprocate with the provision of other related information that will assist the Privacy Commissioner in the performance or exercise of the Privacy Commissioner's functions, duties, or powers under the Privacy Act or any other enactment.

7.2 Before the Privacy Commissioner shares information with the Information Commissioner, the Privacy Commissioner may identify the function, duty, or power of a Participant that would be assisted by the sharing of that information.

7.3 Under section 207 the Privacy Commissioner is able to impose conditions as appropriate which relate to the storage, use, access to and copying, return, and disposal of any information they share with the Information Commissioner.

7.4 Section 207 overrides section 206 of the Privacy Act, which requires the Privacy Commissioner and staff to maintain secrecy in respect of all matters that come to their knowledge in the exercise of their functions under the Privacy Act.

8. SECURITY AND DATA BREACH REPORTING

8.1 The Participants will agree on appropriate security measures in a manner which protects information transfers in accordance with the sensitivity of the information and any classification that is applied by the sender.

8.2 Where confidential material[1] is shared between the Participants, that confidential material 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 OF THE MoU

9.1 The Information Commissioner and the Privacy Commissioner will jointly monitor the operation of this MoU and review it every two years starting on the date of this MoU, 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.

[1] information of a confidential or secret nature, including any information not in the public domain about specific investigations or enforcement actions, or about a party's policy decision making.

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 Information Commissioner or the Privacy Commissioner.

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 through the designated contacts, failing that through the respective Commissioners.

11. DESIGNATED CONTACT POINTS

11.1 Any notice or communication given to a Participant for matters under the MoU will be given in writing and sent to that Participant's designated contact point referred to at clause 11.2.

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

Information Commissioner's Office	**The Office of the Privacy Commissioner**
Name: Adam Stevens Designation: Head of Intelligence	Name: Vanya Vida Designation: Senior Policy Advisor

11.3 The individuals named at clause 11.2 will:

(a) maintain an open dialogue between each other in order to ensure that the MoU remains effective and fit for purpose; and

(b) seek to identify any difficulties in the working relationship between the Participants and proactively seek to minimise the same.

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

Signatories:

Elizabeth Denham **Information Commissioner**	**John Edwards** **Privacy Commissioner**
[redacted] Date: 12 May 2021	[redacted] Date: 12 May 2021