

## Memorandum of Understanding

between:

The Information Commissioner

for

the United Kingdom of Great Britain & Northern Ireland

- and -

The Office of the Australian Information Commissioner

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 for the United Kingdom of Great Britain & Northern Ireland (the "**UK Commissioner**"), and
  - (II) The Office of the Australian Information Commissioner (the "**OAIC**"),
- 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 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 UK Commissioner: the General Data Protection Regulation (the "**GDPR**"); and
  - (b) in the case of the OAIC: the Australian Information Commissioner Act 2010 and the Privacy Act 1988.

- 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 UK COMMISSIONER**

- 2.1 The UK 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 UK 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 UK 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 UK 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 UK 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 UK 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 OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER**

- 3.1 The Office of the Australian Information Commissioner is an independent statutory agency within the Attorney-General's portfolio, and is established by the Australian Information Commissioner Act 2010 ("**AIC Act**").
- 3.2 The Australian Information Commissioner (the "**Australian Commissioner**") is appointed by the Governor-General pursuant to section 14 of the AIC Act.
- 3.3 The Australian Commissioner leads the OAIC as Australia's key independent regulator responsible for promoting and upholding privacy and information access rights.
- 3.4 The Australian Commissioner has a range of statutory functions, duties, obligations and powers and is empowered to take a range of regulatory action under or in relation to parts, or all, of the following legislation (as amended from time to time). This is not an exhaustive list:
  - (a) Australian Information Commissioner Act 2010
  - (b) Privacy Act 1988 (Privacy Act)
  - (c) Freedom of Information Act (FOI Act)
  - (d) Competition and Consumer Act 2010 (in relation to the Consumer Data Right)
  - (e) Crimes Act 1914 (in relation to spent convictions)
  - (f) National Health Act 1953 (in relation to MBS/PBS data matching)
  - (g) Data-matching Program (Assistance and Tax) Act 1990
  - (h) Healthcare Identifiers Act 2010

- (i) My Health Record Act 2012
- (j) Telecommunications Act 1997

The Australian Commissioner's regulatory and enforcement powers include:

- (a) conducting assessments of compliance with the Privacy Act;
- (b) making preliminary inquiries and investigating privacy and FOI complaints;
- (c) conducting Commissioner initiated investigations into acts or practices that may breach the Privacy Act or the FOI Act;
- (d) conducting reviews of FOI decisions
- (e) issuing written notices requiring production of information and documents in relation to an investigation;
- (f) conducting hearings, examining witnesses and directing persons to attend compulsory conferences
- (g) making determinations in relation to privacy investigations, which can include a compensation award payable by the respondent
- (h) issuing proceedings in the Federal Court to enforce determinations
- (i) applying to the Federal Court for a civil penalty order against an agency or organisation

## **2. SCOPE OF CO-OPERATION**

2.1 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 Australia 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.

2.2 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) co-operation in relation to specific projects of interest, including regulation of children's privacy, regulatory sandboxes and artificial intelligence;
- (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.

2.3 This MoU does not impose on either the UK Commissioner or the OAIC 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.

### **3. NO SHARING OF PERSONAL DATA**

- 3.1 The Participants do not intend that this MoU shall cover any sharing of personal data by the Participants.
- 3.2 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 written agreement or arrangement regarding the sharing of such personal data.

### **4. INFORMATION SHARED BY THE UK COMMISSIONER**

- 4.1 Section 132(1) of the DPA 2018 states that the UK Commissioner can only share certain information if she has lawful authority to do so, where that information has been obtained, or provided to, the UK Commissioner in the course of, or for the purposes of, discharging the UK Commissioner's functions, relates to an identifiable individual or business, and is not otherwise available to the public from other sources.
- 4.2 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 UK Commissioner is sharing information with the OAIC are the following circumstances, where:
  - (a) The sharing is necessary for the purpose of discharging the UK 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)).

- 4.3 Before the UK Commissioner shares such information with the OAIC, the UK Commissioner may identify the function of the OAIC with which that information may assist, and assess whether that function of the OAIC could reasonably be achieved without access to the particular information in question.
- 4.4 The UK Commissioner may choose to share certain information with the OAIC only if the OAIC agrees to certain limitations on how it may use that information.

## **5. INFORMATION SHARED BY THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER**

- 5.1 Section 29 of the AIC Act makes unauthorised dealing with information an offence where information is acquired in the course of performing functions or exercising powers for the purposes of an information commissioner function, a freedom of information function or a privacy function.
- 5.2 Further to the framework permitting the sharing of information by the Australian Commissioner with the UK Commissioner, sections 10(2), 11(3) and 12(3) state the Australian Commissioner has the power to do 'all things necessary and convenient to be done' for or in connection with the performance of her functions.
- 5.3 Section 29(2) of the AIC Act sets out the circumstances in which it is not an offence to share information. The OAIC may share information with the ICO in circumstances, where:
- (a) a person records, discloses or otherwise uses the information in the course of performing the same functions or exercising the same powers as those in the course of which the information was acquired; or
  - (b) the person acquires the information for any other lawful purpose; or
  - (c) the person to whom the information relates consents to the recording, disclosure or use of the information.

- 5.4 Provided the Australian Commissioner acts pursuant to the powers and functions set out in the AIC Act and has due regard to the objects of the AIC Act (and any other law) the Australian Commissioner can share information as intended by this MoU.

## **6. SECURITY AND DATA BREACH REPORTING**

- 6.1 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.
- 6.2 Where confidential material is shared between the Participants it will be marked with the appropriate security classification.
- 6.3 Where one Participant has received information from the other, it will seek consent from the other Participant before passing the information to a third party or using the information in an enforcement proceeding or court case.
- 6.4 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.

## **7. REVIEW OF THE MoU**

- 7.1 The UK Commissioner and the OAIC will monitor the operation of this MoU and review it biennially, or sooner if either Participant so requests.
- 7.2 Any issues arising in relation to this MoU will be notified to the designated point of contact for each Participant.
- 7.3 This MoU may only be amended by the Participants in writing and signed by each Participant.

**Signatories:**

<b>James Dipple-Johnstone</b> Deputy Commissioner - Operations	<b>Angelene Falk</b> Australian Information Commissioner and Privacy Commissioner
	
Date: 14 / 1 / 2020	Date: 28 . 01 . 2020 .

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

- 8.1 This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the UK Commissioner or the OAIC.
- 8.2 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.

**9. DESIGNATED CONTACT POINTS**

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

<b>The Information Commissioner for the United Kingdom of Great Britain &amp; Northern Ireland</b>	<b>Office of the Australian Information Commissioner</b>
Name: Adam Stevens	Name: Elizabeth Hampton
Designation: Head of Intelligence	Designation: Deputy Commissioner

- 9.2 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.
- 9.3 Each Participant may change its designated contact point for the purposes of this MoU upon notice in writing to the other Participant.