

Date: 14 July 2022

Memorandum of Understanding

between:

The Information Commissioner

for

The United Kingdom of Great Britain & Northern Ireland

- and -

The Data Protection Commission

of Ireland

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 Data Protection Commission (the "**DPC**"),
- 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 supervision and enforcement cooperation with the aim of providing consistency and certainty.
- 1.3 The Participants acknowledge that they have similar functions and duties concerning the protection of personal data in their respective countries.
- 1.4 The Participants highlight the unique geographical, cultural, social and economic links between their countries, and the importance of consulting on, and taking account of, their respective regulatory activity, where appropriate, in order to better protect the citizens of the United Kingdom and Ireland and support businesses in compliance with laws protecting personal data.
- 1.5 This MoU reaffirms the intent of the Participants to deepen their existing relations and to promote exchanges to assist each other in the regulation of laws protecting personal data.
- 1.6 This MoU sets out the broad principles of collaboration between the Participants and the legal framework governing the sharing of relevant information between them.
- 1.7 Reducing divergences in the regulatory approach taken by the Participants, when addressing similar issues, benefits individuals, industry, and other stakeholders in their respective countries. Whilst having regard to the different laws and regulations of their respective countries as well as their statutory independence, this MoU is intended

to reduce divergences and promote consistency, where possible, in the administration of similar data protection laws.

1.8 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 place either Participant in breach of 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 DPC: all applicable data protection law including, but not limited to, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"), the Irish Data Protection Acts 1988 to 2018, the Law Enforcement Directive (Directive (EU) 2016/680) as transposed in Irish law by the Irish Data Protection Act 2018 ("**Irish DPA**") and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, as amended, and as transposed in Irish law by S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 and the caselaw thereunder.

1.9 The MoU sets out the legal framework for information sharing, but it is for each Participant to determine for themselves, in any case, that any proposed disclosure is compliant with/permitted by 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 UK Data Protection Act 2018 (the "**UK 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) The UK 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 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 UK DPA, UK 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 UK 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 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 DPC

3.1 The DPC is an independent statutory body established pursuant to the Irish DPA and is responsible for upholding the fundamental right of individuals in the European Union (“**EU**”) to have their personal data protected. Accordingly, the DPC is the Irish supervisory authority

responsible for monitoring the application of and enforcing applicable data protection law, including the GDPR, on its territory.

3.2 The DPC has a range of statutory powers which it uses to carry out its functions, including to:

- (a) examine complaints from individuals in relation to potential infringements of data protection law;
- (b) conduct inquiries and investigations regarding potential infringements of data protection law and take enforcement action where necessary;
- (c) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data;
- (d) promote the awareness on the part of controllers and processors of their obligations under the GDPR, including by way of the publication of high-quality guidance and proactive engagement with public and private sector organisations; and
- (e) cooperate with, including the sharing of information with and the provision of mutual assistance to, other EU data protection authorities with a view to ensuring the consistency of application and enforcement of the GDPR, including in the context of the GDPR's cooperation and consistency mechanisms.

4. SCOPE OF CO-OPERATION

4.1 The Participants acknowledge that it is in their common interest to collaborate, where appropriate, 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 individuals within the United Kingdom and Ireland 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 these purposes, 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) joint initiatives in the area of regulatory and technology foresight;
- (d) exchange of information (excluding personal data) involving potential or on-going investigations of organisations in the respective jurisdictions in relation to a potential contravention of personal data protection legislation;
- (e) secondment of staff;
- (f) joint investigations into cross-border personal data incidents involving organisations in both jurisdictions (excluding sharing of personal data);
- (g) convening bilateral meetings at least quarterly or as mutually decided between the Participants; and
- (h) any other areas of cooperation as mutually decided by the Participants.

4.3 For clarity, it is acknowledged that this MoU does not impose any obligation on the Participants to share information with each other or to engage in any form of cooperation. It is further acknowledged that a Participant may require that any cooperation is subject to certain limitations or conditions being agreed between the Participants, for example, in order to avoid breaching applicable legal requirements.

Any such limitations or conditions will be agreed between the Participants on a case-by-case basis.

- 4.4 For the avoidance of doubt, cross-border processing, for the purposes of this MoU, means the processing of personal data which has the potential to impact upon data subjects within the United Kingdom and Ireland. In other words, the terms "cross-border processing" should not be understood as meaning that which has been prescribed by Article 4(23) GDPR.

5. COSTS, EXPENSES AND RESOURCES

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

6. NO SHARING OF PERSONAL DATA

- 6.1 The Participants do not intend that this MoU will cover any sharing of personal data by the Participants.
- 6.2 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 agreement or further arrangements governing the sharing of such personal data.

7. INFORMATION SHARED BY THE UK INFORMATION COMMISSIONER

- 7.1 Section 132(1) of the UK DPA states that the Commissioner can only share certain information if he 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.

7.2 Section 132(2) of the UK DPA 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 DPC 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)).

7.3 Before the Commissioner shares any such information with the DPC, it may be necessary for the Commissioner to identify the function of the DPC with which that information is intended to assist, and assess whether that function of the DPC could reasonably be achieved without access to the particular information in question. Where the Commissioner considers that any such function could reasonably be achieved without access to the information, it will not share the information unless it determines that there are overriding factors which render such sharing to be lawful and appropriate in all the circumstances.

8. INFORMATION SHARED BY THE DPC

8.1 The DPC may, for the purposes of this MoU, share information with the Commissioner where it considers it is necessary and appropriate to do so, subject always to compliance with section 26 of the Irish DPA.

8.2 Nothing in this MoU shall require the sharing of information by the DPC where such sharing might be inconsistent with the DPC's obligations under the GDPR, including the functioning of the cooperation and consistency mechanism.

9. SECURITY AND DATA BREACH REPORTING

9.1 The Participants will use robust measures to protect the confidentiality of any information exchanged between the Participants pursuant to this MoU. Such measures will include appropriate security measures agreed by the Participants to protect such information and will,

amongst other things, require the Participant receiving information (the "**Recipient**") to take into account the sensitivity of the information; any classification that is applied by the Participant who is sending the information to the other Participant (the "**Sender**"); and any other factors relevant to protecting the security of the information.

- 9.2 Where confidential information is shared between the Participants it will be marked with the appropriate security classification by the Sender.
- 9.3 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.
- 9.4 In the event that confidential information obtained from, or shared by, a Sender is wrongfully disclosed or used by a Recipient, the Recipient will bring this to the attention of the Sender without delay.

10. REVIEW OF THE MoU

- 10.1 The Commissioner and the DPC will monitor the operation of this MoU and review it biennially, or sooner if either Participant so requests.
- 10.2 Any issues arising in relation to this MoU will be notified to the designated point of contact for each Participant.
- 10.3 Any amendments to this MoU must be made in writing and signed by each Participant.

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

- 11.1 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 DPC.
- 11.2 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.

12. DESIGNATED CONTACT POINTS

12.1 The following persons will be the designated contact points for the Participants for matters under this MoU:

Information Commissioner's Office	Data Protection Commission
Name: Rory Munro Designation: Head of International Regulatory Cooperation	Name: Alison King Designation: Head of International Affairs Unit

12.2 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.

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

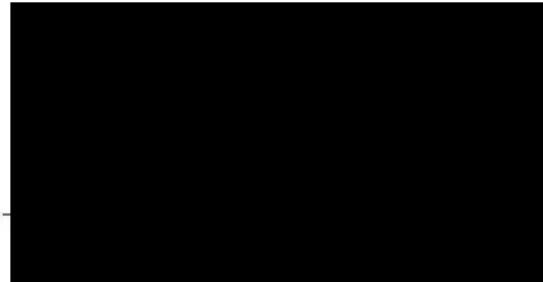
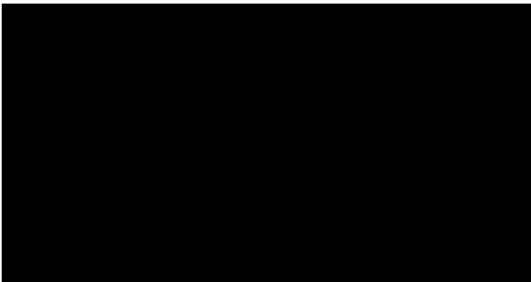
13. ENTRY INTO EFFECT AND TERMINATION

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.

Signatories:

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

**For the Data Protection
Commission of Ireland**



Name: John Edwards

Name: Dale Sunderland

Title: UK Information Commissioner

Title: Deputy Commissioner, Irish
Data Protection Commission

Place: London, UK

Place: London, UK

Date: 14 July 2022

Date: 14 July 2022