Memorandum of Understanding

between

The Information Commissioner

for

The United Kingdom of Great Britain & Northern Ireland

- and -

The Information and Data Protection Commissioner

of

the Republic of Malta

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 Office of the Information and Data Protection Commissioner (the "**IDPC**");

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 cross-border enforcement cooperation in the area of data protection 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, historical, cultural, and economic links between their countries, and the importance of keeping each other informed about their respective regulatory activity in order to better protect the rights and freedoms of the citizens of the United Kingdom and of Malta and support businesses in compliance with laws protecting personal data.

1.5 This MoU reaffirms the intent of the Participants to strengthen 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 The Participants acknowledge the importance of ensuring harmonisation in their regulatory approaches by addressing similar

issues, benefits industry, consumers 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 promote the consistent application of similar data protection laws.

1.8 The Participants confirm that nothing in this MoU should be interpreted as imposing a legal requirement on the participants to co-operate with each other. In particular, there shall be 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 IDPC: Regulation (EU) 2016/679 ("**GDPR**")

1.9 The MoU sets out the legal framework for information sharing. Notwithstanding the non-compulsory nature of any information exchange between the Participants under this MoU, 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 Information Commissioner

2.1 The Commissioner is a corporation sole appointed 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 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) 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 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 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 IDPC

3.1 The IDPC is the national independent supervisory authority responsible for upholding the fundamental right of individuals to have their personal data protected and to monitor the application of data protection law in Malta. The IDPC derives its main functions and powers from the GDPR, as implemented in the Data Protection Act (Chapter 586 of the Laws of Malta) and in the subsidiary legislation issued thereunder.

3.2 The IDPC is also the competent authority responsible for monitoring the application of the following regulatory frameworks in Malta:

(a) Directive 2002/58/EC ("e-Privacy Directive"), as amended by Directive 2009/136/EC and as implemented by virtue of the Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation 586.01);

(b) Directive (EU) 2016/680 ("Law Enforcement Directive"), as implemented in the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations (Subsidiary Legislation 586.08);

(c) Freedom of Information Act (Chapter 496 of the Laws of Malta);

(d) Directive (EU) 2019/1024, as implemented into the Re-Use of Public Sector Information Act (Chapter 546 of the Laws of Malta); and

(e) Directive 2003/4/EC, as implemented into the Freedom of Access to Information on the Environment Regulations (Subsidiary Legislation 549.39).

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 cooperate in a manner that underpins their data-based economies and protect the fundamental rights of citizens of the United Kingdom and of Malta 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 regulatory developments in their respective countries which may have 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 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, strategies, education and training programmes;

(b) implementation of joint research projects;

(c) co-operation in technology and innovation matters which have or may have an impact on data protection, such as, without limitations, artificial intelligence, blockchain, cybersecurity, data science, facial recognition, internet of things, machine learning, privacy enhancing technologies and processing of biometric data. Cooperation in these matters may include the use of sandboxes and, or other analogous tool;

(d) exchange of information (excluding personal data) involving potential or on-going investigations of organisations in the respective jurisdictions in relation to an alleged contravention of personal data protection legislation;

(e) secondment of staff;

(f) joint investigations (excluding sharing of personal data);

(g) convening bilateral meetings as mutually decided between the Participants; and

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

4.3 For clarity, the Participants hereby acknowledge that this MoU does not have any binding legal effect and it shall not impose any obligation

on the Participants to share information with each other or to engage in any form of cooperation.

4.4 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.

5. NO SHARING OF PERSONAL DATA

5.1 The Participants agree that this MoU is not intended to cover any sharing of personal data between them.

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 do so in 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.

6. INFORMATION SHARED BY THE UK INFORMATION COMMISSIONER

6.1 Section 132(1) of the DPA 2018 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.

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 IDPC 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 any such information with the IDPC, it may be necessary for the Commissioner to identify the function of the IDPC with which that information is intended to assist, and assess whether that function of the IDPC 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.

7. INFORMATION SHARED BY THE IDPC

7.1 By virtue of article 50(1)(b) of the GDPR, the IDPC shall take appropriate steps to provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms.

7.2 In terms of article 15(3) of the Data Protection Act, the IDPC may seek the advice of, and may consult with, any other competent authority in the exercise of his functions under the Act and the GDPR.

8. SECURITY AND DATA BREACH REPORTING

8.1 Appropriate security measures will be agreed to protect information that is shared between the Participants. Such measures 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.

8.2 Where confidential material is shared between the Participants it will be marked with the appropriate security classification by the Sender.

8.3 Where a Recipient receives information from a Sender, the Recipient will consult with the Sender and obtain their consent before passing that information to a third party or using the information in an enforcement proceeding or court case, save where the Recipient is prevented from consulting with the Sender or seeking its consent, by applicable laws or regulations.

8.4 Where confidential material 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.

9. REVIEW OF THE MoU

9.1 The Commissioner and the IDPC will monitor the operation of this MoU and review it in the event that either Participant so considers necessary.

9.2 The Participants agree that upon any substantial change to the regulatory framework for which the Participants are respectively responsible, the Participants shall start a consultation process to determine whether this MoU shall be retained as is, amended or terminated. In case the Participants do not find an agreement after six (6) months from the commencement of the consultation process, this MoU shall be terminated ex officio.

9.3 Any issues arising in relation to this MoU will be notified to the designated point of contact for each Participant.

9.4 Any amendments to this MoU shall be made in writing and signed by each Participant.

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 Commissioner or the IDPC.

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	**Office of the Information and Data Protection Commissioner**
Name: Rory Munro Designation: Head of International Regulatory Cooperation	Name: Luana Farrugia Designation: Legal Counsel

11.2 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.

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.

Signatories:

For the Information Commissioner for the United Kingdom of Great Britain and Northern Ireland	**For the Office of the Information and Data Protection Commissioner of the Republic of Malta**
[redacted]	[redacted]
Name: Mr Stephen Bonner	Name: Mr Ian Deguara
Title: Deputy Information Commissioner	Title: Information and Data Protection Commissioner
Place: Sliema, Malta	Place: Sliema, Malta
Date: 23/6/23	Date: 23.06.2023