

MEMORANDUM OF UNDERSTANDING

BETWEEN:

**THE OFFICE OF THE INFORMATION AND DATA PROTECTION
COMMISSIONER OF MALTA**

- AND -

THE ISLE OF MAN INFORMATION COMMISSIONER

1. INTRODUCTION

- 1.1. This Memorandum of Understanding (“MoU”) establishes a framework for cooperation and information sharing between:
- a. the Office of the Information and Data Protection Commissioner (the “IDPC”); and
 - b. the Isle of Man Information Commissioner (the “IOMIC”);

Each referred to as a “Party” and together referred to as the “Parties”.

- 1.2. The Parties recognise the nature of the modern global economy, the increase in circulation and exchange of personal data across borders – particularly across different continents 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 Parties acknowledge that they have similar functions and duties concerning the protection of personal data in their respective jurisdictions.
- 1.4. This MoU reaffirms the intent of the Parties to strengthen their existing relations and to promote exchanges to assist each other in the delivery of their regulatory functions.
- 1.5. This MoU sets out the broad principles of collaboration between the Parties and the legal framework governing mutual assistance including the sharing of relevant information and best practices between them.
- 1.6. The Parties 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.
- 1.7. The Parties confirm that nothing in this MoU should be interpreted as imposing a legal requirement on the Parties to co-operate with each other. In particular, there shall be no

requirement to co-operate in circumstances which would place either Party in breach of their legal responsibilities deriving from the laws which they monitor and enforce.

- 1.8. The MoU sets out the framework for information sharing. Notwithstanding the non-compulsory nature of any information exchange between the Parties under this MoU, it is for each Party to determine for themselves that any proposed disclosure is compliant with the law applicable to them.

2. SCOPE OF COOPERATION

- 2.1. The Parties acknowledge that it is in their common interest to collaborate in accordance with this MoU, in order to:

- a. ensure that the Parties are able to cooperate in a manner that underpins their data-based economies and protect the fundamental rights of citizens of Malta and of the Isle of Man respectively, in accordance with the applicable laws of the Parties' respective jurisdictions;
- b. cooperate with respect to the enforcement of their respective applicable data protection and privacy laws; and
- c. promote a better understanding by each Party of economic and legal conditions and theories relevant to the enforcement of the applicable data protection laws;
- d. communicate as needed to discuss matters of mutual interest and to enhance regulatory co-operation;
- e. consult each other on issues which have significant implications for both Parties; and
- f. keep each other informed of regulatory developments in their respective countries which may have a bearing on this MoU.

- 2.2. For this purpose, the Parties 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 and education 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 Parties;
- h. communication between the parties, as needed, to support the above areas of cooperation; and
- i. any other areas of cooperation as mutually decided by the Parties.

3. THE ROLE AND FUNCTION 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 EU GDPR as implemented in the Malta DPA (Chapter 586 of the Laws of Malta) and in subsidiary legislation issued thereunder.
- 3.2. The IDPC is also the regulator for other main regulatory frameworks, including:

- a. Directive 2002/58/EC (e-Privacy Directive), as amended by Directive 2009/136/EC and as implemented in Subsidiary Legislation 586.01;
 - b. Directive (EU) 2016/680 (Law Enforcement Directive), as implemented in Subsidiary Legislation 586.08;
 - c. the Freedom of Information Act (Chapter 496 of the Laws of Malta); and
 - d. the Re-Use of Public Sector Information Act (Chapter 546 of the Laws of Malta).
- 3.3. The IDPC is vested with extensive investigative powers to properly carry out its functions, which include inter alia the power to request any information required for the performance of its tasks and the prerogative to conduct investigations in the form of audits.
- 3.4. The IDPC has at its disposal a wide range of corrective tools to respond to detected infringements of data protection law. These include inter alia imposing reprimands, administrative fines, processing bans and ordering measures to bring the unlawful processing back into compliance.

4. THE ROLE AND FUNCTION OF THE IOMIC

- 4.1. The IOMIC is established by statute as the Isle of Man's Information Commissioner, functioning as an independent regulator to uphold information rights, promote openness by public bodies and data privacy for individuals.
- 4.2. The IOMIC is empowered to take a range of regulatory actions for breaches of, *inter alia*, the following legislation (as amended from time to time):
- a. The IOM GDPR;
 - b. The GDPR and LED Implementing Regulations 2018 ("Implementing Regulations");
 - c. The Data Protection Act (Application of the GDPR) Order 2018 ("GDPR Order");
 - d. The Data Protection (Application of LED) Order 2018 ("LED Order");

e. The Unsolicited Communications Regulations 2005 ("UCR");

f. The Freedom of Information Act 2015 ("IOM FOI")

4.3. Section 2 of Chapter VI of the IOM GDPR places a broad range of statutory duties on the IOMIC, including monitoring and enforcement of the IOM GDPR, promotion of good practice and adherence to the data protection obligations by those who process personal data in the Isle of Man.

4.4. Schedule 3 to the IOM GDPR also provides the IOMIC with the power to serve enforcement notices and issue monetary penalty notices as above to organisations who breach the UCR. This includes, but is not limited to, breaches in the form of unsolicited marketing which falls within the ambit of the UCR, including automated telephone calls made without consent, telephone calls which have not been screened against the Telephone Preference Service¹, and unsolicited electronic messages.

4.5. The IOMIC's regulatory and enforcement powers include:

- a. conducting assessments of compliance with the IOM GDPR;
- b. issuing information notices requiring individuals, controllers, processors or other persons to provide information in relation to an investigation;
- c. issuing reprimands, warnings and enforcement notices requiring specific actions by a person to resolve infringements (including potential infringements) of Isle of Man data protection legislation and other information rights obligations;
- d. administering fines by way of penalty notices in the circumstances set out in Regulation 112 of the Implementing Regulations;
- e. issuing decision notices detailing the outcome of an investigation under the Isle of Man FOI; and

¹ This service is provided by the UK Information Commissioner's Office, for fixed line and mobile subscribers who do not want to receive unsolicited direct marketing calls and/or faxes. This service is based on the provisions found in the Privacy Regs.

- f. prosecuting criminal offences relating to the protection of personal data before the Courts.

4.6. Article 50 of the IOM GDPR and Regulations 81 to 83 of the Implementing Regulations requires the IOMIC, in relation to third countries and organisations, take appropriate steps to, in an international role, *inter alia*:

- a. develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data, including making agreements with the European Commission or any competent supervisory authority if appropriate,
- b. 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 the significant interests of data subjects,
- c. engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data, and
- d. promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts.

5. COOPERATION AND COMMUNICATION

5.1. Each Party shall appoint a primary contact for all communications and assistance requests under this MoU.

5.2. When requesting assistance in cross-border cooperation of applicable data protection laws, Parties shall ensure that:

- a. requests contain sufficient detail to assess the matter which is subject to the cooperation action, including factual background, type of assistance sought, and any necessary precautions;

b. the intended use of the requested information is clearly specified; and

c. a preliminary assessment is conducted to confirm the request aligns with this MoU and does not impose an undue burden.

5.3. Parties intend to cooperate and exchange relevant information to support ongoing investigations, as appropriate.

5.4. Parties shall promptly notify each other if shared information is found to be inaccurate, incomplete, or outdated.

5.5. Any disputes arising under this MoU shall be addressed through the designated contacts under Section 5.1, and if unresolved, escalated to the heads of the respective Parties.

6. NO SHARING OF PERSONAL DATA

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

6.2. If the Parties wish to share personal data, for example in relation to any cross border personal data incidents involving organisations in both jurisdictions, each Party will do so in compliance with its own applicable data protection laws, which may require the Parties to enter into a written agreement or further arrangements governing the sharing of such personal data.

7. SECURITY AND DATA BREACH REPORTING

7.1. Appropriate security measures will be agreed to protect information that is shared between the Parties. Such measures will, amongst other things, require the Party receiving information (the “**Recipient**”) to take into account the sensitivity of the information; any classification that is applied by the Party who is sending the information to the other Party (the “**Sender**”); and any other factors relevant to protecting the security of the information.

7.2. Information shared under this MoU is to be treated as confidential and will not be further disclosed without the consent of the other Party. Where confidential material is shared between the Parties it will be marked with the appropriate security classification by the Sender.

- 7.3. 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.
- 7.4. 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.

8. REVIEW OF MOU

- 8.1. The Parties will monitor the operation of this MoU and review it in the event that either Party so considers necessary.
- 8.2. The Parties agree that upon any substantial change to the regulatory framework for which the Parties are respectively responsible, the Parties shall start a consultation process to determine whether this MoU shall be retained as is, amended or terminated. In case the Parties do not find an agreement after six (6) months from the commencement of the consultation process, this MoU shall be terminated ex officio.
- 8.3. Any issues arising in relation to this MoU will be notified to the designated point of contact for each Party.
- 8.4. Any amendments to this MoU shall be made in writing and signed by each Party.

9. NON-BINDING EFFECT OF THIS MOU AND DISPUTE SETTLEMENT

- 9.1. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the IDPC or the IOMIC
- 9.2. The Parties 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 or other forum.

10. KEY CONTACTS

- 10.1. The Parties have both identified a key person who is responsible for managing this MoU. Those individuals will maintain an open dialogue between each other in order to ensure 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. ENTRY INTO EFFECT AND TERMINATION

- 11.1. This MoU will come into effect upon its signature by the Parties and remain in effect unless terminated by either Party upon three (3) months' written notice to the other Party.

Signatories:

For the Isle of Man Information
Commissioner


18-September-2025
Alexandra Delaney-Bhattacharya

Isle of Man Information Commissioner

For the Office of the Information and Data
Protection Commissioner of Malta

11

Ian Deguara

Information and Data Protection
Commissioner

18th September 2025