Memorandum of Understanding

between

The Gibraltar Regulatory Authority as

the Information Commissioner for Gibraltar

- and -

The Isle of Man Information Commissioner

for Co-operation in the Regulation of Laws Protecting Personal Data

Definitions

1. '**Personal data**' means any information relating to an identified or identifiable natural person **("data subject")**; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. '**Controller**' means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

3. '**Consent'** means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Introduction

1. This Memorandum of Understanding **("MoU")** establishes a framework for co-operation and information sharing between:

(a) The Gibraltar Regulatory Authority as the Information Commissioner for Gibraltar **(the "GRA")**; and

(b) The Isle of Man Information Commissioner **(the "IOMIC")**,

Each referred to as a **"Party"** and together referred to as the **"Parties"**.

2. The Parties 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 co-operation.

3. The Parties acknowledge that they have similar functions and duties for the protection of personal information in their respective jurisdictions.

4. This MoU reaffirms the intent of the Parties to deepen their existing relations and to promote exchanges to assist each other in the execution of their regulatory functions.

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.

6. The Parties confirm that nothing in this MoU should be interpreted as imposing a requirement on the Parties to co-operate with each other. In particular, there is no obligation to co-operate in circumstances which would breach their legal responsibilities.

7. In the case of the GRA, the Data Protection Act 2004 **(the "Gibraltar DPA")** and/or the Gibraltar General Data Protection Regulation **(the "Gibraltar GDPR")**.

8. In the case of the IOMIC, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data **("Convention 108")** and the Additional Protocol thereto **("Treaty 181")**, the Data Protection Act 2018 **(the "IOM DPA")** and the Data Protection (Application of GDPR) Order 2018 **(the "IOM GDPR")**.

9. This MoU sets out the legal framework for information sharing, but it is for each Party to determine for themselves that any proposed disclosure is compliant with the law applicable to them.

Scope of Co-operation

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

(a) ensure the Parties are able to deliver the regulatory co-operation necessary to underpin their data-based economies and protect the fundamental rights of citizens of Gibraltar and the Isle of Man respectively, in accordance with applicable laws of the Parties' respective jurisdictions;

(b) co-operate with respect to enforcement strategies in relation to their respective applicable data protection and privacy laws;

(c) keep each other informed of developments in their respective jurisdictions having a bearing on this MoU;

11. The Parties may jointly identify one or more areas or initiatives for further co-operation. Such co-operation 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 involving potential or on-going investigations or inquiries of organisations in the respective jurisdictions in relation to an alleged infringement of personal data protection legislation, with the exception of personal data and any other information subject to an obligation of secrecy. For the GRA, section 21 of the Gibraltar Regulatory Authority Act 2000 and any other relevant legislation giving rise to obligations of secrecy and/or confidentiality. For the IOMIC, the IOM GDPR, Convention 108 and Treaty 181 shall apply in this respect;

(e) convening bilateral meetings annually or as mutually decided by the Parties; and

(f) any other areas of co-operation as mutually decided by the Parties;

12. This MoU does not impose on either the GRA or the IOMIC any obligation to co-operate with each other or to share any information. Where a Party 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 the MoU, or (ii) compliance with the request would breach the Parties' legal responsibilities.

The role and function of the GRA

13. The GRA is established by statute as Gibraltar's Information Commissioner, functioning as an independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

14. The GRA is empowered to take a range of regulatory actions for breaches of, inter alia, the following legislation (as amended from time to time):

(a) Gibraltar DPA;

(b) Gibraltar GDPR;

(c) Data Protection (Search and Seizure) Regulations 2006;

(d) Communications (Personal Data and Privacy) Regulations 2006 **(the "Privacy Regs")**;

(e) Freedom of Access to Information on the Environment Regulations 2005 **(the "Gibraltar EIR")**; and

(f) Freedom of Information Act 2018 **(the "Gibraltar FOI").**

15. Article 57 of the Gibraltar GDPR and Section 124 of the Gibraltar DPA place a broad range of statutory duties on the GRA, including monitoring and enforcement of the Gibraltar GDPR and Gibraltar DPA, promotion of good practice and adherence to the data protection obligations by those who process personal data in Gibraltar.

16. The GRA's regulatory and enforcement powers include:

(a) conducting assessments of compliance with the Gibraltar DPA and Gibraltar GDPR;

(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 162 of the Gibraltar DPA;

(e) issuing decision notices detailing the outcome of an investigation under the Gibraltar FOI and Gibraltar EIR; and

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

17. Regulation 31 of the Privacy Regs, also provides the GRA with the power to serve enforcement notices and issue monetary penalty notices as above to organisations who breach the Privacy Regs. This includes, but is not limited to, breaches in the form of unsolicited marketing which falls within the ambit of the Privacy Regs, including automated telephone calls made without consent, telephone calls which have not been screened against the Opt-Out Register [1], and unsolicited electronic messages (Regulations 22, 23 and 24 of the Privacy Regs respectively.)

18. Article 50 of the Gibraltar GDPR requires the GRA to, in relation to third countries and organisations, take appropriate steps to, inter alia:

(a) develop international co-operation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of legislation and practice for the protection of personal data, including legislation and practice relating to jurisdictional conflicts with third countries.

The role and function of the IOMIC

19. The IOMIC is established by statute as the Isle of Man's Information Commissioner, functioning as an independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

[1] This service is provided by the GRA, as the Information Commissioner, 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.

20. 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 (Application of LED) Order 2018 ("Applied LED")**

(d) The Unsolicited Communications Regulations 2005 **("UCR")**;

(e) The Freedom of Information Act 2015 **("IOM FOI");** and

21. 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.

22. 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 Service[2], and unsolicited electronic messages.

23. 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;

[2] 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.

(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

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

24. Article 50 of the IOM GDPR and Regulations 81 – 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.

Information shared between the GRA and the IOMIC

25. The GRA and the IOMIC, during the course of their activities, will receive information from a range of sources. One Party may identify that information held ought to be shared with the other Party as it would assist in performing the functions and responsibilities of the other Party.

26. One Party will share information with the other Party in circumstances where they have determined that it is reasonably necessary to do so. In doing so, the Party which intends to share the information will identify the function of the other Party with which that information may assist and assess whether that function could reasonably be

achieved without access to the particular information in question. Should that be the case, the particular information in question shall not be shared.

27. Where a request for information is received by any of the Parties from a third-party under data protection laws, the receiving Party will seek the views of the other Party where the information being sought by the third-party includes information obtained from, or shared with the receiving Party by, the other Party. However, the decision to disclose or withhold information (and therefore any liability arising out of that decision) remains with the receiving Party as Controller in respect of that data.

28. The Parties shall not exchange any personal data between them on the basis of the procedure established in this section.

Method of exchange

29. Appropriate security measures shall be agreed to protect information transfers between the Parties in accordance with the sensitivity of the information and any classification that is applied by the sender.

Complaint referral

30. In the event that, as a result of preliminary vetting of a complaint, the Party receiving the complaint (the **"Complaint Recipient**") establishes that the other Party is competent to handle the complaint (the **"Competent Party"**), the Complaint Recipient may refer such complaint to the Competent Party; provided that the Complaint Recipient will only refer a complaint to the Competent Party in the event that it has obtained the explicit consent of the data subject who had filed the complaint, and after having informed the same data subject of the possible risks of transferring the data subject's personal data to the Competent Party.

31. The Complaint Recipient which refers a complaint to the Competent Party should provide the Competent Party with all the documents submitted by the data subject filing the complaint and with all information in its possession concerning the complaint.

32. Once the Complaint Recipient refers a complaint to the Competent Party pursuant to the procedure set out herein, it shall cease to handle the complaint so transferred, it should inform the data subject who filed the complaint accordingly and provide him or her with the contact details of the Competent Party.

33. In case the data subject who filed the complaint withdraws his or her explicit consent previously given to the Complaint Recipient to refer the complaint to the Competent Party, the Complaint Recipient should inform the Competent Party without delay.

34. After being informed about the withdrawal of consent by the data subject, the Competent Party should stop processing the data subject's personal data and erase such personal data with immediate effect, unless it has another valid legal ground to continue to process the personal data. If so, the Competent Party should inform the Complaint Recipient about the grounds relied on to continue processing the personal data.

35. Where the data is erased, the Competent Party should confirm with the Complaint Recipient to have stopped processing the data subject's personal data and to have erased the data.

Confidentiality and data breach reporting

36. Material shall be considered confidential when it is identified as such under applicable law or in case the risk of its disclosure is likely to create harm of any nature and degree to any of the Parties and to other stakeholders such as data subjects.

37. Where confidential material is shared between the Parties, the originating Party shall mark it as "CONFIDENTIAL". The Parties shall maintain this marking to any further re-use and adaptation of the material.

38. Where one Party has received information from the other Party, they may use the information solely for the purposes set out in the relevant request for information or as otherwise agreed in writing between the Parties.

39. Where one Party has received information from the other Party, they will obtain the written permission of the other Party before passing the information on to a third party or using the information in an enforcement proceeding or court case.

40. Where confidential material obtained from, or shared by, the originating Party is wrongfully disclosed by the Party holding the information, this Party will bring this to the attention of the originating Party without delay.

41. In accordance with relevant legislation, the GRA and the IOMIC will protect the confidentiality and sensitivity of all confidential material received from the other Party, and maintain effective controls designed to minimise the risk of inappropriate disclosures.

42. The GRA and the IOMIC will liaise where relevant, to the extent permitted by law and having regard to their respective objectives, on responding to enquiries from the public, including Freedom of Information Act requests (GRA) and requests under the IOM FOI (IOMIC) and will consult each other before releasing information originally belonging to the other.

Duration and review of the MoU

43. The Parties will monitor the operation of this MoU and will review it biennially. Should the Parties fail to review the same, subject to paragraph 43 below, the MoU shall nevertheless continue in force as if a review had been conducted and no changes made.

44. Any minor changes to this MoU identified between reviews may be agreed in writing between the Parties.

45. Any issues arising in relation to this MoU will be notified to the key contact for each Party.

46. Either Party may unilaterally terminate this MoU by submitting prior notice to the other Party at any given time. Such termination shall become effective thirty calendar days from the date of submission of said notice.

Non-binding effect of this MoU and dispute settlement

47. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the GRA or the IOMIC.

48. 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.

Key contacts

49. 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.

Signatories

Bradley Tosso
Director of Information Rights and Operations

Iain McDonald
Isle of Man Information Commissioner

Dated this **23rd Day of June 2023**