

MEMORANDUM OF UNDERSTANDING

between the

Jersey Data Protection Authority/Information Commissioner

and

The Isle of Man Information Commissioner

Contents

1.	Definitions	3
2.	Recitals	4-6
3.	Purpose and Principles	7
4.	Scope of co-operation	7-8
5.	Legal basis for information	8-10
6.	Procedure for Assistance	10-11
7.	Investigation and enforcement	11-12
8.	Assessing requests	12
9.	Contact points	13
10.	Costs	13
11.	Confidentiality and data breach reporting	13-14
12.	Retention and disposal of information	14
13.	Consultation	14
14.	Commencement and termination	14
15.	Publication	14

Definitions

In this Memorandum of Understanding, unless the context requires otherwise:

"applicable law"	means any law (statutory, common or customary) applicable to Jersey or the Isle of Man to a matter covered by this MoU;
"Commissioner"	means the Information Commissioner for Jersey (appointed pursuant to Article 5 of the DPAJL 2018);
"Controller"	means the same as defined in Article 1 of the Data Protection (Jersey) Law 2018 and IOM GDPR;
"DPJL 2018"	means the Data Protection (Jersey) Law 2018 (as may be amended from time to time);
"DPAJL 2018"	means the Data Protection Authority (Jersey) Law 2018 (as may be amended from time to time);
"IOM GDPR"	means the legal instruments constituting 'data protection law 2018' as enacted in the Isle of Man;
"FOI Law"	means the Freedom of Information (Jersey) Law 2011 (as may be amended from time to time);
"IOM FOI"	means the Freedom of Information Act 2015 in the Isle of Man;
"GDPR"	means the General Data Protection Regulation (EU) 2016/679;
"IOMIC"	means the Isle of Man Information Commissioner;
"Information Commissioner"	means the Information Commissioner for Jersey (appointed pursuant to Article 5 of the DPAJL 2018);
"JDPA"	means the Jersey Data Protection Authority;
"JOIC"	means the Jersey Office of the Information Commissioner, which is the operating name of the JDPA;
"MoU"	means this memorandum of understanding;
"Parties"	means the JDPA/Information Commissioner and the IOMIC;
"Person"	means a natural person, legal entity, partnership or unincorporated association;
"Receiving Party"	means either party receiving information from the other under this MoU;
"Sending Party"	means either party when sending information to the other under this MoU;

Memorandum of Understanding ("MoU")

between the

**Jersey Data
Protection Authority
("JDPA")/Information
Commissioner)**

-and-

**The Isle of Man
Information
Commissioner
("IOMIC")**

Recitals

- A. The JDPA is a statutory body established under the Jersey DPAJL 2018 to act as Jersey's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals. The JDPA consists of the Authority, the Information Commissioner and the staff of the office. The operational name for the Information Commissioner and staff of the office is the JOIC.
- B. The JDPA is empowered to take a range of regulatory action for breaches of the DPJL 2018, the DPAJL 2018 and by the Information Commissioner in respect of the FOI Law.
- C. Part 4 of the DPAJL 2018 places a broad range of statutory duties on the JDPA, including monitoring and enforcement of the DPJL 2018, 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 enforcement regime under the FOI Law.
- D. The JDPA (and Information Commissioner's) regulatory and enforcement powers include:
- a. conducting assessments of compliance with the DPJL 2018, the DPAJL 2018 and the FOI Law;
 - 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 Article 26 of the DPAJL 2018;
 - e. issuing decision notices detailing the outcome of an investigation under the FOI Law;
 - f. certifying contempt of court should a public authority fail to comply with an information notice, decision notice or enforcement notices under the FOI Law;

- g. investigating potential regulatory matters including liaising with the Jersey Financial Services Commission where appropriate; and
 - h. investigating potential criminal offences and liaising with the States of Jersey Police where appropriate.

- E. Article 15 of the DPAJL 2018 requires the JDPA, amongst other things, to:
 - a. develop international cooperation 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, 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 co-operation 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 with third countries.

- F. 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.

- G. 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**)

- H. 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.

- I. 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.

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

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.

Purpose and Principles

1. This MoU establishes a framework for cooperation and information sharing between the Parties. It sets out the broad principles of collaboration and the legal framework governing the sharing of relevant information and intelligence between the parties. The shared aims of this MoU are to enable closer working between the Parties, including the exchange of appropriate information, to assist them in discharging their regulatory functions.
2. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the JDPA or the IOMIC. This MoU does not modify or supersede any laws or regulatory requirements in force in, or applying in, Jersey or the Isle of Man. This MoU does not affect any arrangements under other MoUs.
3. The Parties acknowledge that they may only provide information under this MoU if permitted or not prevented under applicable laws, regulations and/or requirements.
4. The Parties have determined that they do not exchange enough personal data to warrant entering into a separate data sharing agreement, but this will be kept under review.

Scope of co-operation

5. 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 Jersey and the Isle of Man respectively, in accordance with applicable laws of the Parties' respective jurisdictions;
 - b. co-operate with respect to the enforcement of 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;
 - d. recognise parallel or joint investigations or enforcement actions by the Parties as priority issues for co-operation.
6. The Parties may jointly identify one or more areas for 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 of organisations in the Parties' respective jurisdictions in relation to a contravention of data protection legislation;
 - e. joint investigations into cross-border personal data incidents involving organisations in both jurisdictions;
 - f. convening bilateral meetings annually or as mutually decided by the Parties;
 - g. any other areas of co-operation as mutually decided by the Parties.
7. Information exchange will normally be responsive and will specifically relate to concerns as they arise. The parties may also wish to proactively share emerging themes or trends.
8. There will be a two-way sharing of information, which may be volunteered by one regulator to the other or provided in response to a particular request.
9. This MoU does not impose on either the JDPA 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 a) it is outside the scope of the MoU, or b) compliance with the request would breach the Parties' legal responsibilities.

Legal basis for sharing information

Information shared by the IOMIC to the JDPA

10. The IOMIC, during the course of their activities, will receive information from a range of sources, including personal data. The IOMIC will process all personal data in accordance with the principles of the IOM GDPR and all other applicable legislation. The IOMIC may identify that information held, which may include personal data, ought to be shared with the JDPA as it would assist in performing the functions and responsibilities of the JDPA.

11. Section 91 of the Isle of Man Implementing Regulations states that information obtained by the IOMIC in the course of, or for the purposes of, discharging their functions can only be shared with others if there is lawful authority to do so. Section 91 of the Isle of Man Implementing Regulations sets out the circumstances in which the IOMIC will have lawful authority to share that personal data with the JDPA.
12. The IOMIC will be permitted to share information with the JDPA in circumstances where they have determined that it is reasonably necessary to do so in furtherance of one of the grounds outlined in para.18. In doing so, the IOMIC will identify the function of the JDPA with which that information may assist and assess whether that function could reasonably be achieved without access to the particular information in question. In particular, where the information proposed for sharing with the JDPA amounts to personal data, the IOMIC will consider whether it is necessary to provide it in an identifiable form in order for the JDPA to perform their functions, or whether disclosing it in an anonymised form would suffice. The IOMIC will also be permitted to share information in matters where the IOMIC and JDPA both have jurisdiction as a result of cross-border processing, where there has been a request for mutual assistance and where there is a joint investigation being conducted.

Information shared by the JDPA to the IOMIC

13. The JDPA, during the course of its activities, will receive information from a range of sources, including personal data. It processes all personal data in accordance with the principles of the DPJL 2018 and all other applicable legislation. The JDPA may consider that certain of the information it holds, which may include personal data, ought to be shared with the IOMIC as it would assist them in performing their functions and responsibilities and acting in the public interest.
14. Art.8 of the DPAJL 2018 states that the JDPA can only share confidential information with others if there is lawful authority to do so. In this context, the information will be considered confidential if it has been obtained, or provided to, the JDPA in the course of, or for the purposes of, discharging its functions, relates to an identifiable individual or business, and is not otherwise available to the public from other sources. This therefore includes, but is not limited to, personal data. Art.8(2) of the DPAJL 2018 sets out the circumstances in which the JDPA will have the lawful authority to share that confidential information with the IOMIC.
15. The JDPA will therefore be permitted to share information with the IOMIC in circumstances where it has determined that it is reasonably necessary to do so in furtherance of one of those grounds outlined at paragraph 22. In doing so, the JDPA will identify the function of the IOMIC with which that information

may assist and assess whether that function could reasonably be achieved without access to the information in question. Where the information proposed for sharing with the IOMIC amounts to personal data the JDPA will consider whether it is necessary to provide it in an identifiable form for the IOMIC to perform its functions, or whether disclosing it in an anonymised form would suffice. The JDPA will also be permitted to share information in matters where the JDPA and JOIC both have jurisdiction as a result of cross-border processing, where there has been a request for mutual assistance and where there is a joint investigation being conducted.

16. Unless otherwise stated, information exchanged between the JDPA/Information Commissioner and the IOMIC under the provisions of this MoU is for intelligence purposes only and should it be required formally as evidence or for use in an investigation then the appropriate formal request must be made.
17. Where a request for information is received by either party under data protection laws the recipient of the request will seek the views of the other party where the information being sought under the request includes information obtained from, or shared by, the other party. However, the decision to disclose or withhold the information (and therefore any liability arising out of that decision) remains with the party in receipt of the request as Controller in respect of that data.

Procedure for Assistance

18. Requests for the provision of information or other assistance will be made in writing or – in urgent cases – made orally and, unless otherwise agreed, confirmed in writing within five business days. To facilitate assistance, the Requesting Party should specify in any written request:
 - a. a description of the information or other assistance requested;
 - b. if information is provided by the Requesting Party for confirmation or verification, the information and the kind of confirmation or verification sought;
 - c. the purpose for which the information or other assistance is sought; and
 - d. to whom, if anyone, onward disclosure of information provided to the Requesting Party is likely to be necessary and the purpose such disclosure would serve.
19. The Parties will notify each other without delay, if they become aware that information shared under this MoU is not accurate, complete, and up to date.
20. The Parties will use their best efforts to resolve any disagreements related to co-operation that may arise under this MoU through the contacts designated

under this section and, failing resolution in a timely manner, by discussion between the Information Commissioner and the IOMIC.

Investigation and enforcement

21. The Parties recognise that there are areas in which they have complementary functions and powers. They will therefore endeavour to ensure that in these cases, the most appropriate body or bodies will commence and lead investigations. To the extent permitted by law and having regard to their respective powers, expertise, and resources, they will seek to ensure that in cases of investigations, the Parties will notify each other of significant developments where the other is likely to have an interest. Where appropriate, the parties will discuss the steps they propose to take and ensure co-ordination takes place in a timely manner, where possible, allowing for a proper exchange of views.
22. The Parties may refer a matter for action if the other body is considered more appropriate to deal with the matter. Any such referral will include the action sought and the legal powers it considers are available to the other. Where the other party determines not to proceed, an explanation will be provided, where possible.
23. Where the Parties agree that an investigation should be carried out by both of them, it will usually be appropriate that both investigations proceed in parallel. However, in appropriate circumstances, they will consider whether the particular facts of the matter, as they are known at that time, suggest that one party's investigation should proceed before the others.
24. Where information exchanged between the JDPA/Information Commissioner and the IOMIC indicates that the subject of the information is of interest to both parties (for example where regulatory breaches under both sets of regulatory laws are suspected) a case conference may be called to ensure that the maximum, and appropriate, use of the information is made. In relevant cases, the JDPA/Information Commissioner, and the IOMIC, may seek the involvement of a representative of their respective jurisdiction's prosecuting authority – His Majesty's Attorney General(s) – in the case conference.
25. Where either party carries out any subsequent investigation and proceedings alone, that party will keep the other regularly updated on material aspects of the progress of the investigation.
26. If a decision is made by either party to take action against a subject, the JDPA/Information Commissioner and the IOMIC should consider whether it is possible and would be appropriate to co-ordinate publication of applicable

enforcement announcements so that both parties publish the outcome of their investigations simultaneously. In any event, the JDPA/Information Commissioner and the IOMIC will endeavour to give the other appropriate notice of any press release or other public statement it intends to make relating to enforcement cases in which the other may have an interest, no later than 24 hours prior to publication unless there are overriding reasons which prevent or delay such notice.

27. Relevant JDPA and IOMIC staff will, where appropriate, seek to maintain general awareness and understanding of each other's functions and needs and will liaise with each other to ensure that issues are appropriately identified.

Assessing requests

28. Each request for assistance will be assessed on a case-by-case basis by the Receiving Party to determine whether assistance can be provided under the terms of this MoU. In any case where the request cannot be fulfilled in part or whole, the Receiving Party may be asked to provide the reasons for not granting the assistance and consider whether there may be other assistance which can be given by itself.

29. In deciding whether and to what extent to fulfil a request, the Requested Party may take into account:

- a. whether the request conforms with this MoU;
- b. whether the provision of assistance would be so burdensome as to disrupt the proper performance of the Receiving Party's functions;
- c. whether it would be otherwise contrary to the public interest to give the assistance sought;
- d. any other matters specified by applicable laws, regulations, and requirements (in particular those relating to confidentiality and professional secrecy, data protection and privacy, and procedural fairness);
- e. whether complying with the request may otherwise be prejudicial to the performance by the Receiving Party of its functions; and
- f. the security arrangements, including cyber defences, that will apply to information disclosed under this MoU.

30. The Parties recognise that assistance may be denied in whole or in part for any of the reasons mentioned in clause 30 in the discretion of the Receiving Party.

Contact points

31. The JDPA and IOMIC will designate a primary contact for the purposes of any communications under the MoU. Those 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 work to minimise same.

Costs

32. If the cost of fulfilling a request is likely to be substantial, the Receiving Party may, as a condition of agreeing to give assistance under this MoU, require the Requesting Party to make a contribution to costs, although the parties will work to ensure information is disclosed to the other in the public interest.

Confidentiality and breach reporting

33. 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 Sending Party.

34. All non-public information shared under this MoU will be marked as such by the Sending Party and marked with the appropriate security classification.

35. Where one party has received information from the other, it will consult (where permissible) with the other party before passing the information to a third party or using the information in an enforcement proceeding or court case and notify the Sending Party if it anticipates a legally enforceable demand for disclosure of the information.

36. Similarly, the Receiving Party will notify the Sending Party if any legally enforceable demand for disclosure of the information is received, unless this is not practicable because of urgency or prohibited by law.

37. If requested by the Sending Party in relation to a legally enforceable demand for disclosure of the information, the Receiving Party shall assert any legal exemptions or privileges against disclosure on behalf of the Sending Party.

38. If it is not practicable to notify the Sending Party of the receipt of a legally enforceable demand for disclosure of the information, assume the Sending Party will wish to assert any legal exemptions or privileges against disclosure.

39. Where confidential material obtained from, or shared by, the Sending Party is wrongfully disclosed by the Receiving Party holding the information, this party will bring this to the attention of the Sending Party immediately. This is in addition to obligations to report a personal data breach under the DPJL 2018 where personal data is contained in the information disclosed.

40. In accordance with relevant legislation, the JDPA and IOMIC will protect the confidentiality and sensitivity of all unpublished and other confidential information received from the other, and maintain effective controls designed to minimise the risk of inappropriate disclosures.

41. The JDPa and 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 requests and will consult each other before releasing information originally belonging to the other.

Retention and disposal of information

42. The JDPa and IOMIC acknowledge that any information provided under this MoU must not be retained for longer than is reasonably required to fulfil the purpose for which it was sought or for longer than permitted under applicable data protection legislation. As soon as practicable after any information supplied under this MoU is no longer required, the relevant party will dispose of it in a secure manner.

Consultation

43. The Parties will keep the operation of this MoU under review and will consult where necessary with a view to improving its operation and resolving any matters,

44. Both Parties will consult in matters relating to any difficulties that may arise in relation to specific request made pursuant to this MoU (e.g., where a request may be denied, or if it appears that responding to a request will involve a substantial cost).

Commencement, and Termination

45. This MoU will take effect once both Parties have signed it.

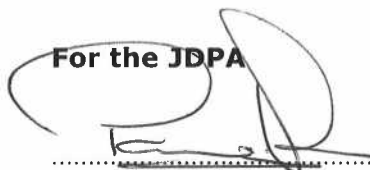
46. This MoU will continue to have effect until terminated by either Party giving 30 days' advance written notice to the other Party. It may be amended by agreement, in writing.

47. In the event of the termination of this MoU, information shared under this MoU will remain subject to clauses 37 to 47.

Publication

48. Either, or both, or the parties may make a copy of this MoU or the text of it, publicly available.

For the JDPa



Paul Vane
Information Commissioner
1 November 2024

For IOMIC



Alexandra Delaney-Bhattacharya
Information Commissioner
1 November 2024