

Date: 28 October 2024

Memorandum of Understanding

Between:

The Data Protection Authority/
Information Commissioner

for

the Bailiwick of Jersey

- and -

The Information Commissioner

for

The United Kingdom of Great Britain &
Northern Ireland

for Cooperation in the Regulation of
Laws Protecting Personal Data

Definitions

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

"applicable law"	means any law (statutory, common or customary) applicable to Jersey and the UK to a matter covered by this MoU;
"Controller"	means the same as defined in Article 1 of the Data Protection (Jersey) Law 2018;
"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);
"FOI Law"	means the Freedom of Information (Jersey) Law 2011 (as may be amended from time to time);
"GDPR"	means the General Data Protection Regulation (EU) 2016/679;
"UK Commissioner"	means the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland;
"Jersey 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;

"Participants"	means the JDPA/Jersey Information Commissioner and the UK Commissioner;
"Person"	means a natural person, legal entity, partnership or unincorporated association;
"Receiving Participant"	means either Participant receiving information from the other under this MoU;
"Sending Participant"	means either Participant when sending information to the other under this MoU;
"UK DPA"	means the Data Protection Act 2018;
"UK GDPR"	means the United Kingdom General Data Protection Regulation.

1. Purpose and Principles

- 1.1 This Memorandum of Understanding (“**MoU**”) establishes a framework for cooperation between the Participants:
- (I) Jersey Data Protection Authority/Information Commissioner (the “**JDPA/Jersey Information Commissioner**”); and
 - (II) The Information Commissioner for the United Kingdom of Great Britain & Northern Ireland (the “**UK Commissioner**”).
- 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 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, and economic links between their countries, and the importance of consulting on, and taking account of, their respective regulatory activity in order to better protect the individuals within the scope of data protection and privacy legislation in Jersey and the United Kingdom 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 of appropriate information 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 and intelligence between them.
- 1.7 This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either Participants. This MoU does not modify or supersede any laws or regulatory requirements in force in, or applying in Jersey and the UK. This MoU does not affect any arrangements under other MoUs.

- 1.8 The Participants acknowledge that they may only provide information under this MoU if permitted or not prevented under applicable laws, regulations and/or requirements.
- 1.9 The Participants 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. It is for each Participant to determine for themselves that any proposed disclosure is compliant with the law applicable to them.

2. Role and function of the JDPA/Jersey Information Commissioner

- 2.1 The JDPA is a statutory body established under the 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 Jersey Information Commissioner and staff of the office is the JOIC.
- 2.2 The JDPA is empowered to take a range of regulatory action for breaches of the DPJL 2018, the DPAJL 2018 and by the Jersey Information Commissioner in respect of the FOI Law.
- 2.3 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.
- 2.4 The JDPA (and Jersey 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.

2.5 Article 15 of the DPAJL 2018 requires the JPA, 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.

3. Role and function of the UK Information Commissioner

3.1 The Commissioner is responsible for promoting and enforcing data protection law in the UK and upholding information rights in the public interest. The Commissioner is the Supervisory Authority appointed under the UK General Data Protection Regulation (UK GDPR) and for the purposes set out in the Data Protection Act 2018, which supports and supplements the UK GDPR.

3.2 The Commissioner is empowered to take a range of regulatory action for breaches of the following legislation (as amended from time to time):

- (a) UK DPA;
- (b) UK GDPR;
- (c) Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**");
- (d) Freedom of Information Act 2000 ("**UK FOIA**");
- (e) Environmental Information Regulations 2004 ("**UK EIR**");
- (f) Environmental Protection Public Sector Information Regulations 2009 ("**UK 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 Regulations 2018 ("**NIS Regulations**"); and
- (k) Electronic Identification, Authentication and Trust Services Regulation ("**eIDAS**").

3.3 Under Article 57 of the UK GDPR and Section 115 of the UK DPA, the UK 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 as outlined below.

3.4 The UK Commissioner's regulatory and enforcement powers include, but are not limited to:

- (a) conducting assessments of compliance with the UK DPA, UK GDPR, PECR, eIDAS, the NIS Regulations 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.

3.5 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).

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 deliver the regulatory cooperation necessary in their data-based economies and protect the fundamental rights of individuals within the scope of data protection and privacy legislation in Jersey and the UK 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 this purpose, the Participants may jointly identify one or more areas or initiatives for cooperation. Such cooperation may include, but is not limited to:

- (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 (excluding personal data) involving potential or on-going investigations of organisations in the Participants' 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 Participants;
- (g) any other areas of co-operation as mutually decided by the Participants.

4.3 Information exchange will normally be responsive and will specifically relate to concerns as they arise. The Participants may also wish to proactively share emerging themes or trends.

4.4 This MoU does not impose on either the JDPA or the UK Commissioner any obligation to co-operate with each other or to share any information. Where a Participant 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 Participant's legal obligations. 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 do not intend that this MoU will cover any sharing of personal data by the Participants.
- 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 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.

6. Information shared between the Participants

Information shared by the UK Commissioner to the JDPA

- 6.1 The UK Commissioner, during the course of his activities, will receive information from a range of sources, including personal data. The UK Commissioner will process all personal data in accordance with the principles of the UK GDPR, the UK DPA and all other applicable legislation. The UK Commissioner 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.
- 6.2 Section 132(1) of the UK DPA states that the UK Commissioner can only share certain information if he has lawful authority to do so, where that information has been obtained, or provided to, the UK Commissioner in the course of, or for the purposes of, discharging his functions, relates to an identifiable individual or business, and is not otherwise available to the public from other sources.
- 6.3 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 UK Commissioner is sharing information with the JDPA are the following circumstances, where:
- (a) The sharing is necessary for the purpose of discharging the UK 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)).
- 6.4 Before the UK Commissioner shares any such information with the JDPA, it may be necessary for the UK Commissioner to identify the function of the JDPA with which that information is intended to assist, and assess whether that function of the JDPA

could reasonably be achieved without access to the particular information in question. Where the UK 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.

Information shared by the JDPA to the UK Commissioner

- 6.5 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 UK Commissioner as it would assist them in performing their functions and responsibilities and acting in the public interest.
- 6.6 Article 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 has been obtained, or provided to, the JDPA in the course of, or 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. Article 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 UK Commissioner.
- 6.7 Before the JDPA shares any such information with the UK Commissioner, it may be necessary for the JDPA to identify the function of the UK Commissioner with which that information is intended to assist, and assess whether that function of the UK Commissioner could reasonably be achieved without access to the particular information in question. Where the JDPA 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.
- 6.8 Unless otherwise stated, information exchanged between the Participants 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.
- 6.9 Where a request for information is received by either Participant under data protection laws, the recipient of the request will seek the views of the other

Participant where the information being sought under the request includes information obtained from, or shared by, the other Participant. However, the decision to disclose or withhold the information (and therefore any liability arising out of that decision) remains with the Participant in receipt of the request as Data Controller in respect of that data.

7. Procedure for Assistance

7.1 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 as soon as reasonably practicable. To facilitate assistance, the Requesting Participant should specify in any written request:

- (a) a description of the information or other assistance requested;
- (b) if information is provided by the Requesting Participant 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 Participant is likely to be necessary and the purpose such disclosure would serve.

7.2 The Participants will notify each other without delay, if they become aware that information shared under this MoU is not accurate, complete, and up-to-date.

8. Investigation and enforcement

8.1 The Participants 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 Participants will notify each other of significant developments where the other is likely to have an interest. Where appropriate, the Participants 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.

- 8.2 The Participants 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 Participant determines not to proceed, an explanation will be provided, where possible.
- 8.3 Where the Participants 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 Participant's investigation should proceed before the others.
- 8.4 Where information exchanged between the JDPA/Jersey Information Commissioner and the UK Commissioner indicates that the subject of the information is of interest to both Participants (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/Jersey Information Commissioner may seek the involvement of a representative of Jersey's prosecuting authority – Her Majesty's Attorney General – in the case conference.
- 8.5 Where either Participant carries out any subsequent investigation and proceedings alone, that Participant will keep the other regularly updated on material aspects of the progress of the investigation.
- 8.6 If a decision is made by either Participant to take action against a subject, the JDPA/Jersey Information Commissioner and the UK Commissioner should consider whether it is possible and would be appropriate to co-ordinate publication of applicable enforcement announcements so that both Participants publish the outcome of their investigations simultaneously. In any event, the JDPA/Jersey Information Commissioner and the UK Commissioner 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.

9. Assessing requests

- 9.1 Each request for assistance will be assessed on a case-by-case basis by the Receiving Participant 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 Participant 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.
- 9.2 In deciding whether and to what extent to fulfil a request, the Requested Participant may take into account:
- (a) whether the request confirms with this MoU;
 - (b) whether the provision of assistance would be so burdensome as to disrupt the proper performance of the Receiving Participant 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 Participant of its functions; and
 - (f) the security arrangements, including cyber defences, that will apply to information disclosed under this MoU.
- 9.3 The Participants recognise that assistance may be denied in whole or in part for any of the reasons mentioned above in the discretion of the Receiving Participant.

10. Confidentiality and data breach reporting

- 10.1 Appropriate security measures shall be agreed to protect information that is shared between the Participants in accordance with the sensitivity of the information and any classification that is applied by the Sending Participant.
- 10.2 All non-public information shared under this MoU will be marked as such by the Sending Participant and marked with the appropriate security classification.

As soon as practicable after any information supplied under this MoU is no longer required, the relevant Participant will dispose of it in a secure manner.

12. Review of the MOU

12.1 The JDPA and UK Information Commissioner will monitor the operation of this MoU and review it if either Participant so requests.

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

12.3 Any amendments to this MoU must be made in writing and signed by each Participant.

13. Non-binding effect of this MoU and dispute settlement

13.1 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 UK Commissioner.

13.2 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.

14. Designated contact points

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

Jersey Data Protection Authority	Information Commissioner's Office
Name:	Name: Rory Munro
Designation:	Designation: Head of International Regulatory Cooperation

14.2 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.

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

15. Entry into effect and termination

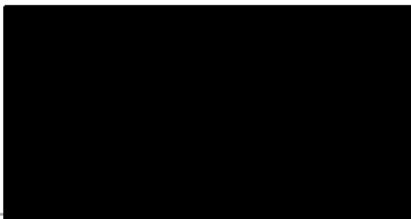
15.1 This MoU will come into effect upon its signature by the Participants and remain in effect unless terminated by either Participant upon two months' written notice to the other Participant.

15.2 In the event of the termination of this MoU, information shared under this MoU will remain subject to Sections 10 and 11.

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

Signatories:

**For the Jersey Data Protection
Authority/Jersey Information
Commissioner**

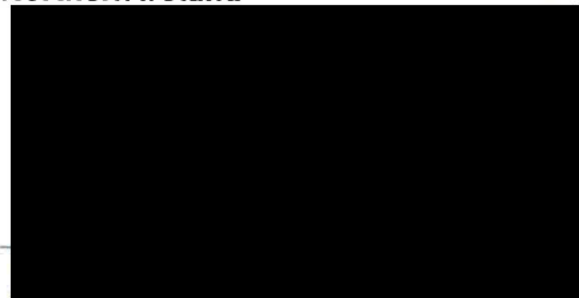


Name: Mr Paul Vane

Title: Information Commissioner

Date: 28/10/24.

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



Name: Mr John Edwards

Title: Information Commissioner

Date: 28/10/24

