Date: 17 September 2025

Memorandum of Understanding

between:

The Information Commissioner

for

The United Kingdom of Great Britain & Northern Ireland

- and -

The Data Protection Authority

for

The Bailiwick of Guernsey

for Cooperation in the Regulation of Laws Protecting Personal Data

1. INTRODUCTION

1.1 This Memorandum of Understanding ("**MoU**") establishes a framework for cooperation between

(I) The Information Commissioner for the United Kingdom of Great Britain and Northern Ireland (the "**Information Commissioner**") and

(II) The Data Protection Authority for The Bailiwick of Guernsey (the "**Data Protection Authority**")

together referred to as the "**Participants**".

1.2 The Participants recognise the nature of the modern global economy, the increase in circulation and exchange of personal data across borders, the increasing complexity of information technologies, and the resulting need for 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 individuals within scope of the applicable data protection and privacy laws of the United Kingdom and The Bailiwick of Guernsey and support organisations 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 exchange of information, experience, and best practice 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 Reducing divergence between the regulatory approaches taken by the Participants, when 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 avoid divergences and promote consistency in the administration of similar data protection laws.

1.8 The Participants confirm that nothing in this MoU should be interpreted as imposing a requirement on the Participants to co-operate with each other. In particular, there is no requirement to co-operate in circumstances which would place either Participant in breach of their legal responsibilities, including:

(a) in the case of the Information Commissioner: the United Kingdom General Data Protection Regulation and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025; and

(b) in the case of the Data Protection Authority: the Data Protection (Bailiwick of Guernsey) Law, 2017 (as amended).

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

2. ROLE AND FUNCTIONS OF THE INFORMATION COMMISSIONER

2.1 The Information Commissioner is a corporation sole appointed under the Data Protection Act 2018 to act as the UK's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

2.2 The Information Commissioner is empowered to take a range of regulatory action under the following legislation (as amended from time to time):

(a) Data Protection Act 2018 ("DPA"), as amended by the Data (Use and Access) Act 2025 ("DUAA");

(b) United Kingdom General Data Protection Regulation ("UK GDPR"), as amended by DUAA;

(c) Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), as amended by DUAA;

(d) Freedom of Information Act 2000 ("FOIA");

(e) Environmental Information Regulations 2004 ("EIR");

(f) Environmental Protection Public Sector Information Regulations 2009 ("INSPIRE Regulations");

(g) Investigatory Powers Act 2016;

(h) Re-use of Public Sector Information Regulations 2015;

(i) Enterprise Act 2002;

(j) Network and Information Systems Regulations 2018 ("NIS Regulations"); and

(k) the UK eIDAS Regulations ("eIDAS")[1].

2.3 The Information Commissioner has a broad range of statutory duties, including monitoring and enforcing data protection laws, and promoting good practice and adherence to data protection obligations by those who process personal data. These duties sit alongside those relating to the other enforcement regimes.

2.4 The Information Commissioner's regulatory and enforcement powers include:

(a) conducting assessments of compliance with the 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;

[1] The UK eIDAS Regulation is Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (UK eIDAS). Following the UK withdrawal from the EU the eIDAS Regulation was adopted into UK law and amended by The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019). In addition, the existing UK trust services legislation, The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (2016 No.696) was also amended. Taken together, these regulations are referred to in this MoU as the UK eIDAS Regulations.

(c) issuing Enforcement Notices, Warnings, Reprimands, practice recommendations and other orders requiring specific actions by an individual or organisation to resolve breaches (including potential breaches) of data protection legislation and other information rights obligations;

(d) administering fines by way of Penalty Notices in the circumstances set out in section 152 of the DPA;

(e) administering fixed penalties for failing to meet specific obligations (such as failing to pay the relevant fee to the Information Commissioner);

(f) issuing Decision Notices detailing the outcome of a case under FOIA or EIR;

(g) certifying contempt of court should an authority fail to comply with an Information Notice, Decision Notice or Enforcement Notice under FOIA or EIR; and

(h) prosecuting criminal offences before Courts.

2.5 Regulation 31 of PECR, as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, also provides the Information Commissioner with the power to serve Enforcement Notices and issue Monetary Penalty Notices as above to organisations who breach PECR. This includes, but is not limited to, breaches in the form of unsolicited marketing which fall within the ambit of PECR, including automated telephone calls made without consent, live telephone calls which have not been screened against the Telephone Preference Service, and unsolicited electronic messages (Regulations 19, 21 and 22 of PECR respectively).

3. ROLE AND FUNCTIONS OF THE DATA PROTECTION AUTHORITY

3.1 The Data Protection Authority is a body corporate established under the Data Protection (Bailiwick of Guernsey) Law, 2017 to act as the Bailiwick's independent regulator to administer and enforce data protection law and other associated legislation and uphold information rights.

3.2 The Data Protection Authority is empowered to take a range of regulatory action under the following legislation (as amended from time to time):

(a) The Data Protection (Bailiwick of Guernsey Law, 2017 ('DPL');

(b) The Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018 ('DPLEO')

(c) The Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018 ('DPGP')

(d) The Data Protection (International Cooperation and Assistance) (Bailiwick of Guernsey) Regulations, 2018 ('DPICA')

(e) European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance, 2004 ('ECIPD') (and the Alderney and Sark equivalent ordinances)

3.3 The Data Protection Authority has a broad range of statutory duties, including monitoring and enforcing data protection laws, and promoting good practice and adherence to data protection obligations by those who process personal data. These duties sit alongside those relating to the other enforcement regimes.

3.4 The Data Protection Authority's regulatory and enforcement powers include:

(a) conducting assessments of compliance with the DPL, DPLEO, DPGP, DPICA, ECIPD (sections 68 and 69 of the DPL);

(b) issuing information notices requiring individuals, controllers or processors to provide information in relation to any legitimate activity of the Data Protection Authority (schedule 7, paragraph 1 of the DPL);

(c) issuing determinations as to whether or not a controller or processor has breached or is likely to breach an operative provision (sections 71 and 72 of the DPL);

(d) issuing enforcement orders, warnings, reprimands and words of advice in relation to breach determinations (section 73 of the DPL).;

(e) administering fines by way of an order (section 74 of the DPL). Such an order may also require a controller or processor to undertake specific actions related to the matter investigated;

3.5 Sections 27 and 28 of the ECIPD, also provides the Data Protection Authority with the power to exercise its enforcement functions and issue sanctions as above to organisations who breach the ECIPD.

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 to underpin their data-based economies and protect the fundamental rights of individuals within the scope of the applicable data protection and privacy laws of the United Kingdom and the Bailiwick of Guernsey;

(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:

(a) sharing of experiences and exchange of best practices on data protection policies, education and training programmes;

(b) implementation of joint research projects;

(c) exchange of information (excluding personal data) about potential or on-going investigations of organisations in relation to a potential contravention of personal data protection legislation impacting both jurisdictions;

(d) work shadowing, placements, and secondment of staff;

(e) joint investigations into organisations in relation to a potential contravention of personal data protection legislation impacting both jurisdictions (excluding sharing of personal data);

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

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

4.3 For clarity, it is acknowledged that this MoU does not impose any obligation on the Participants to share information with each other or to engage in any other form of cooperation. It is further acknowledged that a Participant may require that any cooperation is subject to certain limitations or conditions being agreed between the Participants, for example, in order to avoid breaching applicable legal requirements. Any such limitations or conditions will be agreed between the Participants on a case-by-case basis.

5. NO SHARING OF PERSONAL DATA

5.1 The Participants 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, each Participant will ensure compliance with its own applicable data protection laws, which may require the Participants to enter into a written agreement or further arrangements governing the sharing of such personal data.

6. INFORMATION SHARED BY THE INFORMATION COMMISSIONER

6.1 Section 132(1) of the DPA states that the Information Commissioner can only share certain information if he has lawful authority to do so, where that information has been obtained by, or provided to, the Information Commissioner in the course of, or for the purposes of, discharging the Information Commissioner's functions, relates to an identifiable individual or business, and is not otherwise available to the public from other sources.

6.2 Section 132(2) of the DPA sets out the circumstances in which the Information Commissioner will have the lawful authority to share that information. In particular, the Information Commissioner may share information with the Data Protection Authority with lawful authority where:

(a) the sharing is necessary for the purpose of discharging the Information Commissioner's functions (section 132(2)(c) of the DPA); or

(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) of the DPA).

6.3 Before the Information Commissioner shares any such information in accordance with this MoU the Information Commissioner will identify and document the function of the Information Commissioner with which the sharing of that information is intended to assist, and assess whether that function could reasonably be achieved without sharing the particular information in question. Where the Information Commissioner considers that any such function could reasonably be achieved without sharing the information, the Information Commissioner will not share the information unless the Information Commissioner determines that there are overriding factors which render such sharing to be lawful and appropriate in all the circumstances.

7. INFORMATION SHARED BY THE DATA PROTECTION AUTHORITY

7.1 Section 90(1) of the DPL states that a designated official of the Data Protection Authority cannot use or disclose information gained in the course of their duties without the consent of any identifiable person.

7.2 Section 91(1) of the DPL sets out the exceptions to the confidentiality offered by Section 90. In particular, a designated official of the Data Protection Authority may share information gathered in the course of their duties with the Information Commissioner where the sharing is necessary for:

- the exercising or performing of any function conferred or imposed on the designated official by the DPL; or
- enabling or assisting a competent supervisory authority to exercise or perform functions conferred or imposed by or under a comparable foreign enactment.

7.3 Section 61(g) of the DPL states that a function of the Data Protection Authority is to cooperate with, including share information and provide mutual assistance to, other competent supervisory authorities with a view to ensuring that the DPL is applied and enforced in a manner equivalent to the GDPR and the Law Enforcement Directive.

7.4 In addition, Section 65(b) of the DPL states that the Data Protection Authority must, as far as is practicable, 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.

7.5 Before the Data Protection Authority shares any such information in accordance with this MoU the Data Protection Authority will identify and document the function of the Data Protection Authority with which the sharing of that information is intended to assist, and assess whether that function could reasonably be achieved without sharing the particular information in question. Where the Data Protection Authority considers that any such function could reasonably be achieved without sharing the information, the Data Protection Authority will not share the information unless the Data Protection Authority determines that there are overriding factors which render such sharing to be lawful and appropriate in all the circumstances

8. SECURITY AND DATA BREACH REPORTING

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

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

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

8.6 Where confidential material obtained from, or shared by, a Sender is wrongfully disclosed or used by a Recipient, the Recipient will bring this to the attention of the Sender without delay.

9. REVIEW OF THE MoU

9.3 The Information Commissioner and the Data Protection Authority will monitor the operation of this MoU and review it if either Participant so requests.

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

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

10. NON-BINDING EFFECT OF THIS MoU AND DISPUTE SETTLEMENT

10.3 This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the Information Commissioner or the Data Protection Authority.

10.4 The Participants will settle any disputes or disagreement relating to or arising from this MoU amicably through consultations and negotiations in good faith without reference to any international court, tribunal or other forum.

11. DESIGNATED CONTACT POINTS

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

Information Commissioner's Office	**The Data Protection Authority (ODPA)**
Name: Rory Munro **Designation:** Head of International Regulatory Cooperation	**Name:** Lawrence West **Designation:** Domestic/International Partnerships Lead

11.4 The above individuals will maintain an open dialogue between each other in order to ensure that the MoU remains effective and fit for purpose. They will also seek to identify any difficulties in the working relationship and proactively seek to minimise the same.

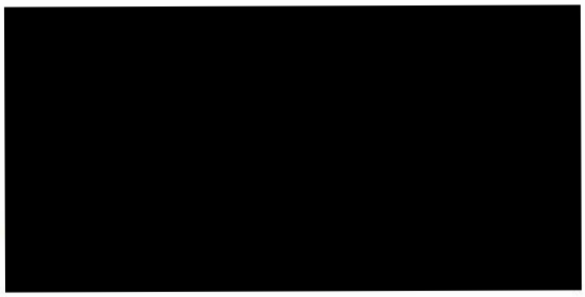
11.5 Each Participant may change its designated contact point for the purposes of this MoU upon notice in writing to the other Participant.

12. ENTRY INTO EFFECT AND TERMINATION

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

Signatories:

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



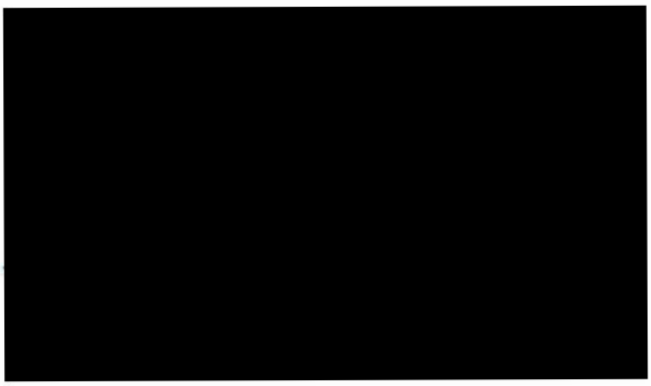
Name: John Edwards

Title: Information Commissioner

Place: Seoul, Republic of Korea

Date:

For the Data Protection Authority for the Bailiwick of Guernsey



Name: Brent R Homan

Title: Data Protection Commissioner

Place: Seoul, Republic of Korea

Date: