Date: 16 September 2025

Memorandum of Understanding

between:

The Information Commissioner

for

The United Kingdom of Great Britain & Northern Ireland

- and -

The Privacy Commissioner of Canada

for Cooperation in the Enforcement of Laws Protecting Personal Data and Privacy

The Privacy Commissioner of Canada ("Privacy Commissioner") and the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland ("Information Commissioner") (together, the "Participants"):

RECOGNIZING 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;

RECOGNIZING the unique 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 Canada and support organisations in compliance with laws protecting personal data (or personal information)[1];

RECOGNIZING that reducing divergence between the regulatory approaches taken by the Participants, when addressing similar issues, benefits members of the public, businesses and other stakeholders in their respective countries and that whilst having regard to the different laws and regulations of their respective countries, as well as their statutory independence, this Memorandum of Understanding ("MoU") is intended to promote consistency in the application of internationally-recognized principles of data protection;

RECOGNIZING that Article 50 of the *United Kingdom General Data Protection Regulation* says the Information Commissioner shall take appropriate steps to, amongst other things, develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

RECOGNIZING that section 23.1 of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("PIPEDA") authorizes the Privacy Commissioner to share information with authorities from other countries that have responsibilities relating to the protection of personal information in the private sector;

RECOGNIZING that the Participants have similar functions and duties concerning the protection of personal data in their respective countries;

[1] The terms "personal data" and "personal information" refer to the same concept and are used interchangeably throughout this MoU.

RECOGNIZING 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; and

RECOGNIZING that nothing in this MoU requires the Participants to provide assistance in the enforcement of laws protecting personal data, in particular if such assistance is prohibited by their respective national laws or enforcement priorities;

HAVE REACHED THE FOLLOWING UNDERSTANDING:

1. INTRODUCTION

1.1 This MoU establishes a framework for cooperation between the Participants. It sets out the broad principles of collaboration between the Participants and the legal framework governing the sharing of relevant information between them.

1.2 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, 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 Privacy Commissioner: PIPEDA and any associated regulations.

2. DEFINITIONS

2.1 For the purposes of this MoU,

(a) "Applicable Privacy Laws" means the laws and regulations of the Participant's country, the enforcement of which have the effect of protecting personal data (or personal information). In the case of the Privacy Commissioner, "Applicable Privacy Laws" means Part 1 of PIPEDA and any associated regulations. 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*; as well as any amendments to the Participants' Applicable Privacy Laws, and such other laws or regulations as the Participants may from time to time jointly decide in writing to be an Applicable Privacy Law for purposes of this MoU;

(b) "Covered Privacy Contravention" means conduct that would be in contravention of one of the Applicable Privacy Laws of a Participant's country and that is the same or

substantially similar to conduct that would be in contravention of one of the Applicable Privacy Laws of the other Participant's country;

(c) "Person" means any natural person or legal entity, including any corporation, unincorporated association, or partnership;

(d) "Request" means a request for assistance under this MoU;

(e) "Requested Participant" means the Participant from whom assistance is sought under this MoU, or who has provided such assistance;

(f) "Requesting Participant" means the Participant seeking or receiving assistance under this MoU.

3. ROLE AND FUNCTIONS OF THE INFORMATION COMMISSIONER

3.1 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.

3.2 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")[2].

3.3 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.

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

(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;

(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

---

[2] 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.

(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 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).

4. ROLE AND FUNCTIONS OF THE PRIVACY COMMISSIONER

4.1 The Privacy Commissioner is appointed under the *Privacy Act*, R.S.C. 1985, C. P-21, and is an independent Agent of Parliament.

4.2 The Privacy Commissioner has a broad range of statutory duties, including overseeing compliance with PIPEDA, Canada's federal private-sector privacy law.

4.3 The Privacy Commissioner's powers under PIPEDA include:

a) conducting investigations in respect of complaints;

b) initiating complaints;

c) summoning and enforcing the appearance of persons and compelling them to give oral or written evidence under oath;

d) entering any premises occupied by an organisation;

e) receiving breach reports;

f) issuing reports of findings and recommendations; and

g) appearing before the Federal Court in applications under PIPEDA.

4.4 The Privacy Commissioner is also required to promote, by any means that they consider appropriate, the purposes of Part 1 of PIPEDA, including by:

a) developing and conducting information programs to foster public understanding and recognition of the purposes of Part 1 of PIPEDA;

b) undertaking and publishing research related to the protection of personal information; and

c) encouraging organisations to develop detailed policies and practices, including organisational codes of practice.

5. SCOPE OF COOPERATION

5.1 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 Privacy Laws of the United Kingdom and Canada;

(b) Cooperate with respect to the enforcement of their respective Applicable 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 cooperation.

5.2 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 privacy and data protection policies, and education and training programmes;

(b) Implementation of joint research projects;

(c) Cooperation in key areas of interest such as biometrics, artificial intelligence and children's privacy;

(d) Exchange of information (excluding personal data) about potential or on-going investigations of organisations in relation to a Covered Privacy Contravention;

(e) Virtual work shadowing, placements, and short- or long-term secondment of staff;

(f) Joint investigations into cross border matters involving both jurisdictions (excluding sharing of personal data);

(g) Convening bilateral meetings as mutually decided between the Participants; and

(h) Any other areas of cooperation as mutually decided by the Participants.

5.3 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 be 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.

6. NO SHARING OF PERSONAL DATA (PERSONAL INFORMATION)

6.1 The Participants do not intend that this MoU will cover any sharing of personal data (personal information) by the Participants.

6.2 If the Participants wish to share personal data, each Participant will ensure compliance with its own Applicable Privacy Laws, which may require the Participants to enter into a further written agreement governing the sharing of such personal data.

7. INFORMATION SHARED BY THE INFORMATION COMMISSIONER

7.1 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.

7.2 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 Privacy Commissioner 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).

7.3 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 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.

8. INFORMATION SHARED BY THE PRIVACY COMMISSIONER

8.1 Subsection 23.1(1) of PIPEDA states that the Privacy Commissioner can only disclose information to any person or body who, under the legislation of a foreign state, has functions and duties similar to those of the Privacy Commissioner with respect to the protection of personal information; or responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of Part 1 of PIPEDA.

8.2 Pursuant to section 23.1(2) of PIPEDA, the Privacy Commissioner is authorized to disclose information that they believe

(a) would be relevant to an ongoing or potential investigation or proceeding in respect of a contravention of the laws of a foreign state that address conduct that is substantially similar to conduct that would be in contravention of Part 1 of PIPEDA; or

(b) is necessary to disclose in order to obtain from the person or body information that may be useful to an ongoing or potential investigation or audit under Part 1 of PIPEDA.

8.3 The Privacy Commissioner may only disclose information to the person or body referred to in section 8.1 if the Privacy Commissioner has entered into a written arrangement with that person or body that

(a) limits the information to be disclosed to that which is necessary for the purpose set out in paragraph 8.2 (a) or (b);

(b) restricts the use of the information to the purpose for which it was originally shared; and

(c) stipulates that the information be treated in a confidential manner and not be further disclosed without the express consent of the Privacy Commissioner.

8.4 The Privacy Commissioner will not share confidential information unless it is for the purpose set out in paragraph 5.2 (d) or (f); or it is necessary for making a request for assistance from the other Participant regarding information that may be useful to an ongoing or potential investigation or audit under Part 1 of PIPEDA.

9. PROCEDURES RELATING TO MUTUAL ASSISTANCE

9.1 Each Participant will designate a primary contact for the purposes of requests for assistance and other communications under this MoU.

9.2 In requesting assistance in procedural, investigative and other matters involved in the enforcement of Applicable Privacy Laws across borders, Participants will ensure that:

(a) requests for assistance include sufficient information to enable the Requested Participant to determine whether a request relates to a Covered Privacy Contravention and to take action in appropriate circumstances. Such information may include a description of the facts underlying the request and the type of assistance sought, as well as an indication of any special precautions that should be taken in the course of fulfilling the request;

(b) requests for assistance specify the purpose for which the information requested will be used; and

(c) prior to requesting assistance, Participants perform a preliminary inquiry to ensure that the request is consistent with the scope of this MoU and does not impose an excessive burden on the Requested Participant.

9.3 Participants intend to communicate and cooperate with each other, as appropriate, about matters that may assist ongoing investigations.

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

9.5 Subject to section 10, Participants may, as appropriate and subject to their Applicable Privacy Laws, refer complaints to each other, or provide each other notice of possible Covered Privacy Contraventions of the Applicable Privacy Laws of the other Participant's country.

10. LIMITATIONS ON ASSISTANCE AND USE

10.1 The Requested Participant may exercise their discretion to decline a request for assistance, or limit or condition their cooperation, in particular where it is outside the scope of this MoU, or more generally where it would be inconsistent with domestic laws, or important interests or priorities. The Requesting Participant may request the reasons for which the Requested Participant declined or limited assistance.

10.2 A Participant will not use any information obtained from the other Participant for purposes other than those for which the information was originally shared.

11. CONFIDENTIALITY

11.1 Information shared under this MoU will be treated as confidential.

11.2 Where one Participant receives information from the other Participant, they will consult with the Participant who shared the information and obtain their express consent before passing that information to a third party or using the information in an enforcement proceeding or court case, save where the Participant is prevented from consulting with the other Participant or seeking their consent, by applicable laws or regulations.

11.3 The Participants will oppose, to the fullest extent possible consistent with their countries' laws, any application by a third party for disclosure of confidential information or materials received from the other Participant, unless that Participant provides express consent to their release. The Participant who receives such an application will promptly notify the Participant that provided them with the confidential information of the third-party application for disclosure.

12. SECURITY, DATA BREACH REPORTING AND RETENTION

12.1 The Participants will agree on appropriate security measures to protect information that is shared between them. Such measures will, amongst other things, require the Participant receiving information 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; and any other factors relevant to protecting the security of the information.

12.2 Where confidential material is shared between the Participants it will be marked with the appropriate security classification by the Participant sharing it.

12.3 Where confidential material obtained from, or shared by, one Participant is subject to unauthorized use or disclosure while in the custody of the other Participant, the Participant who becomes aware of the breach will bring this to the attention of the Participant who originally shared the information without delay.

12.4 Information received under this MoU will not be retained for longer than is required to fulfil the purpose for which it was shared or than is required by the Requesting Participant's country's laws.

12.5 The Participants will use best efforts to return any information that is no longer required if the Requested Participant makes a written request at the time it is shared that such information be returned. If no request for return of the information is made, the Requesting Participant will dispose of the information using methods prescribed by the Requested Participant or if no such methods have been prescribed, by other secure methods, as soon as practicable after the information is no longer required.

13. MONITORING, REVIEW AND AMENDMENT OF THE MoU

13.1 The Participants will monitor the operation of this MoU and review it if either Participant so requests.

13.2 The Participants will maintain an open dialogue with 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 these.

13.3 Any issues arising in relation to this MoU will be communicated to the primary contact for each Participant designated under section 9.1. Participants will use their best efforts to resolve any disagreements related to cooperation that may arise

under this MoU through these primary contacts, and, failing resolution in a reasonably timely manner, by discussion between the Participants themselves.

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

13.5 Any amendments to this MoU will be made in writing and signed by each Participant.

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

14.1 Nothing in this MoU is intended to:

a) create binding obligations, or affect existing obligations under international law, or create obligations under the laws of the Participants' countries;

b) prevent a Participant from seeking assistance from or providing assistance to the other Participant pursuant to other agreements, treaties, arrangements, or practices;

c) affect any right of a Participant to seek information on a lawful basis from a Person located in the territory of the other Participant's country, nor is it intended to preclude any such Person from voluntarily providing legally obtained information to a Participant; or

d) create obligations or expectations of cooperation that would exceed a Participant's jurisdiction.

14.2 The Participants will settle any dispute 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.

15 ENTRY INTO EFFECT AND DURATION OF COOPERATION

15.1 This MoU will come into effect upon its signature by the Participants and supersedes any previous MoU signed between the Participants.

15.2 Assistance in accordance with this MoU will be available concerning Covered Privacy Contraventions occurring before as well as after this MoU is signed.

15.3 This MoU will remain in effect unless terminated by either Participant upon 60 days' written notice to the other Participant.

15.4 On termination of this MoU, the Participants will, in accordance with section 11.1, maintain the confidentiality of any information communicated to them by the other Participant in accordance with this MoU, and return or destroy, in accordance with section 12.5, information obtained from the other Participant.

Signed in duplicate, in the English and French languages, each version being equally authentic. In case of a conflict of interpretation between the two versions, the English version will prevail. Any notice given under or in connection with this MoU will be in English.

Signatories:

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

[redacted]

Name: John Edwards

Title: Information Commissioner

Place: Seoul

Date: 16/09/25

For the Privacy Commissioner of Canada

[redacted]

Name: PHILIPPE DUFRESNE

Title: COMMISSIONER

Place: Seoul

Date: 16-09-25