Memorandum of Understanding

between

The Swiss Federal Data Protection and Information Commissioner

and

The Information Commissioner for The United Kingdom of Great Britain & Northern Ireland

for

the Facilitation of International Co-operation in the Field of Data Protection

The Swiss Federal Data Protection and Information Commissioner (FDPIC)

and

The Information Commissioner for The United Kingdom of Great Britain & Northern Ireland (ICO) hereinafter referred to individually as "Participant", or collectively as "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 on protection of personal data with the aim of providing consistency and certainty,

Recognizing that Art. 58 paragraph 1 letter b of the Swiss Federal Data Protection Act of 25 September 2020 confers upon the FDPIC the power to work with foreign authorities that are responsible for data protection,

Recognizing that Article 50 of the United Kingdom General Data Protection Regulation requires the Information Commissioner to 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 the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy, the Global Privacy Enforcement Network's Action Plan and the International Enforcement Coordination Framework of the Global Privacy Assembly call for the development of cross-border information sharing mechanisms and enforcement cooperation arrangements; and that such information sharing and enforcement cooperation are essential elements to ensure privacy and data protection compliance, serving a substantial public interest,

Acknowledging that they have similar functions and duties concerning the protection of personal data in their respective jurisdictions,

Highlighting the unique geographical, cultural, linguistical 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 the scope of data protection and privacy legislation and ensure compliance with laws protecting personal data in Switzerland and the United Kingdom of Great Britain & Northern Ireland,

have reached the following understanding:

1. OBJECTIVES

1.1 This MoU sets out the intent of the Participants to establish a framework for cooperation and to deepen their existing relations and to promote exchanges to assist each other in the application of laws protecting personal data.

1.2 This MoU sets out the broad principles of collaboration between the Participants and reaffirms the legal framework governing the sharing of relevant information between them. **It does not impose any obligation on the Participants** to share information with each other or to collaborate, in particular where such disclosure or collaboration would allegedly breach their legal responsibilities or applicable national laws, as referenced in Annex 1, or the separation of competences between authorities at national or international level.

2. SCOPE OF CO-OPERATION

2.1 For the purpose of cooperation, the Participants may jointly identify one or more areas. 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 and possible joint publications;

(c) co-operation in international groups and fora, including exchange of information on topics of shared interest;

(d) evaluation of common positions to strengthen impact in discussions within international groups and fora and the global dialogue on data protection and privacy;

(e) exchange of information (excluding personal data) involving potential or on-going investigations of organisations in the respective jurisdictions in relation to a contravention of personal data protection legislation;

(f) joint investigations into cross border personal data incidents involving organisations in 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.

2.2 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 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, limitations of budget or staff or in order to avoid breaching applicable legal requirements or the overstepping of competences at national or international level.

2.3 It is acknowledged that this MoU does not impose any obligation to jointly finalise or conclude any cooperation project started between the Participants under this MoU.

3. SHARING OF INFORMATION, CONFIDENTIALITY, SECURITY AND DATA BREACH REPORTING

3.1 The Participants do not expect this MoU to cover any sharing of information (in particular personal data) by the Participants, unless there is a legal basis for such disclosure and the disclosure is required for the achievement of the intended purposes defined in this MoU.

3.2 Appropriate confidentiality and security measures, taking into account the state of the art for such measures and the laws protecting personal data in the Participants' respective countries, should be agreed to protect information that is shared between the Participants. The Participant receiving such information (the "Recipient") is expected, amongst other things, 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.

3.3 Prior to disclosing information, the Sender may require the Recipient to enter into written arrangements governing the sharing of such information. The Recipient should not use information received by the Sender for any purpose other than specified in this MoU.

3.4 Classified government information should not be shared between the Participants.

3.5 Where the Recipient receives information from the Sender, the Recipient is expected to consult with the Sender and obtain its 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.

3.6 Where information obtained from, or shared by, the Sender is disclosed or used by the Recipient, the Recipient is expected to bring this to the attention of the Sender without delay and inform the Sender of the full circumstances of the disclosure and the information that has been disclosed as soon as possible after such disclosure has been made.

4. REVIEW OF THE MOU

4.1 Each of the Participants may monitor the operation of this MoU and review it at any time if either Participant so requests.

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

4.3 Any amendments to this MoU should be made in writing and signed by each Participant.

5. NON-BINDING EFFECT OF THIS MOU AND DISPUTE SETTLEMENT

5.1 This MoU is a statement of intent that does not give rise to any legally binding obligations on the part of either the FDPIC or ICO.

5.2 The Participants should 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.

6. DESIGNATED CONTACT POINTS

6.1 The following persons should be the designated contact points for the Participants for matters under this MoU:

Caroline Gloor Scheidegger (FDPIC) Head of the Directorate of International Relations	Rory Munro (ICO) Head of International Regulatory Cooperation

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

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

7. COSTS

Each Participant in this MoU is expected to bear its own costs of cooperation.

Signed in duplicate in Seoul on 18 September 2025 in the English language, each version being equally valid.

The Swiss Federal Data Protection and Information Commissioner (FDPIC)	The Information Commissioner for The United Kingdom of Great Britain & Northern Ireland (ICO)
Adrian Lobsiger, Commissioner	John Edwards, Commissioner

Annex 1

Applicable National Laws

I. Swiss Federal Data Protection and Information Commissioner
   a. Art. 13 Right to Privacy of the Federal Constitution of the Swiss Confederation
   b. Swiss Federal Act on Data Protection 2020 ("FADP")
   c. Swiss Federal Ordinance on Data Protection 2022 ("DPO")
   d. Swiss Federal Ordinance on Data Protection Certification ("DPCO")
   e. Swiss Federal Act on Freedom of Information in the Administration 2004 ("FoIA")
   f. Swiss Federal Ordinance on Freedom of Information in the Administration 2006 ("FoIO")

II. Information Commissioner's Office
   a. Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 ("DUAA");
   b. United Kingdom General Data Protection Regulation, as amended by DUAA;
   c. Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), as amended by DUAA;
   d. Freedom of Information Act 2000;
   e. Environmental Information Regulations 2004;
   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; and
   k. the UK eIDAS Regulations.