Date: 31 October 2024

Memorandum of Understanding

between:

The Information Commissioner

for

The United Kingdom of Great Britain & Northern Ireland

- and -

Autoriteit Persoonsgegevens

of

The Netherlands

for Cooperation in the Regulation of Laws Protecting Personal Data

ico.
Information Commissioner's Office

1. Introduction

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

(I) The Information Commissioner (the "**Commissioner**") and

(II) The Autoriteit Persoonsgegevens, Data protection authority of The Netherlands, hereafter: ("**AP**"),

together referred to as the "**Participants**". Any reference to the Commissioner shall include his statutory successors.

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. The Participants record in this MoU their shared commitment to openness in the exercise of their powers and duties.

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 the scope of the applicable data protection and privacy laws of the United Kingdom and the Netherlands 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 exchanges 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 divergences in the regulatory approach 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 but not limited to:

(a) in the case of the Commissioner: the retained EU law version of the General Data Protection Regulation ((EU) 2016/679 ("UK GDPR")); and

(b) in the case of the AP: the Algemenene Verordening Gegevensbescherming ((EU) 2016/679 "AVG")), Uitvoeringswet Algemene Verordening Gegevensbescherming (*Stb.* 2018, 144, (UAVG)), Wet bescherming persoonsgegevens (*Stb.* 2000, 301 (Wbp)), Wet justitiële en strafvorderlijke gegevens *Stb.* 2021, 559 (Wjsg)), Algemene wet bestuursrecht (Awb).

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. THE ROLE AND FUNCTIONS OF THE INFORMATION COMMISSIONER

2.1 The Commissioner is a corporation sole appointed under the Data Protection Act 2018 (the "**DPA**") 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 Commissioner is empowered to take a range of regulatory action for breaches of the following legislation (as amended from time to time):

(a) Data Protection Act 2018 ("DPA");

(b) UK GDPR;

(c) Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR");

(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) Security of Network and Information Systems Directive ("NIS Directive"); and

(k) Electronic Identification, Authentication and Trust Services Regulation ("eIDAS").

2.3 The 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.

2.4 The Commissioner's regulatory and enforcement powers include:

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

2.5 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).

3. THE ROLE AND FUNCTIONS OF THE AP

3.1 The AP has legal personality and sole appointed under the Uitvoeringswet Algemene Verordening Gegevensbescherming 2018 ("**UAVG**") to supervise the processing of personal data in accordance with the provisions of and pursuant to the General Data Protection Regulation (GDPR) or the law.

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

(a) Uitvoeringswet Algemene Verordening Gegevensbescherming ("UAVG");

(b) Wet bescherming Persoonsgegevens ("Wbp");

(c) Wet justitiële en strafvorderlijke gegevens (Wjsg);

(d) Algemene wet bestuursrecht ("Awb");

3.3 The AP is competent to carry out the tasks and exercise the powers laid down in Articles 57 and 58 of the GDPR.

3.4 Pursuant to Article 15 of the UAVG, the AP is also authorised to perform the tasks and exercise the powers conferred on the AP on the basis of the GDPR.

4. SCOPE OF CO-OPERATION

4.1 The Participants acknowledge that it is in their common interest to collaborate on matters within their shared regulatory remits 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 the applicable data protection and privacy laws of the United Kingdom and The Netherlands respectively;

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

(d) secondment of staff;

(e) joint investigations into cross border personal data incidents involving organisations in both jurisdictions (excluding sharing of personal data);

(f) convening bilateral meetings at least quarterly or 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, 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 BY THE UK INFORMATION COMMISSIONER

6.1 Section 132(1) of the DPA 2018 states that the Commissioner can only share certain information if he has lawful authority to do so, where that information has been obtained, or provided to, the Commissioner in the course of, or for the purposes of, discharging the 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 2018 sets out the circumstances in which the Commissioner will have the lawful authority to share that information. Of particular relevance when the Commissioner is sharing information with the AP are the following circumstances, where:

(a) The sharing is necessary for the purpose of discharging the 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)).

6.3 Before the Commissioner shares any such information with the AP, it may be necessary for the Commissioner to identify the function of the AP with which that information is intended to assist, and assess whether that function of the AP could reasonably be achieved without access to the particular information in question. Where the 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.

7. **INFORMATION SHARED BY THE AP**

7.1 Article 2:5 paragraph 1 of the Awb states that any person who is involved in the performance of tasks of the AP, when given access to information of which they know is confidential, or are reasonably to know so, and who is not already subject to a duty of confidentiality by virtue of office, appeal or statutory regulation in respect of that data, is obliged to maintain the confidentiality of such data, except in so far as any legal requirement obliges him to communicate or the need for communication arises from their tasks.

7.2 Based on article 2:5 paragraph 2 Awb, this also applies to institutions and persons belonging to them or employed therein which are involved by an administrative body in the performance of its duties, and to

institutions and related or employed persons carrying out a task conferred by or under the law.

7.3 Article 9 of the Ambtenarenwet provides that the official and the former official shall be obliged to maintain the confidentiality of what was brought to their knowledge in connection with their duties, in so far as that obligation follows from the nature of the case.

8. SECURITY AND DATA BREACH REPORTING

8.1 Appropriate security measures will be agreed to protect information that is shared between the Participants.

8.2 Where confidential material (information that is (i) confidential in nature, and (ii) disclosed in circumstances that give rise to a duty of confidentiality) is shared between the Participants it will be marked appropriately by the sender.

8.3 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, unless the disclosure is required on the basis of law or court order.

8.4 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. RETENTION OF INFORMATION

9.1 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.

9.2 The Participants will use best efforts to return any information that is no longer required if the Requested Participant makes a written request that such information be returned at the time it is shared. 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.

10. COSTS

10.1 Without prejudice to any separate written agreement or arrangement or unless otherwise mutually decided in writing by the Participants, each Participant will bear its own costs and expenses in implementing this MoU.

11. REVIEW OF THE MoU

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

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

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

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

12.1 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.
d) Create obligations or expectations of cooperation that would exceed a Participant's jurisdiction.

12.2 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.

13. DESIGNATED CONTACT POINTS

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

Information Commissioner's Office	**Autoriteit Persoonsgegevens**
Name: Rory Munro Designation: Head of International Regulatory Cooperation	Name: Yasha Holtuin Designation: Senior Adviser International Policy and Transfers

13.2 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.

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

14. 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. However, prior to providing such notice, the Participants should aim to consult with each other.

Signatories:

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

[redacted]

Name: John Edwards

Title: Information Commissioner

Place: St Helier, Jersey

Date: 31 October 2024

For the Autoriteit Persoonsgegevens of the Netherlands

[redacted]

Name: Katja Mur

Title: Board Member

Place: St Helier, Jersey

Date: 31 October 2024