

## Memorandum of Understanding between the Information Commissioner and the Centre for Data Ethics and Innovation

### Introduction

1. This Memorandum of Understanding ("**the MoU**") establishes a framework for cooperation and information sharing between the Information Commissioner ("**the Commissioner**") and the Centre for Data Ethics and Innovation ("**CDEI**"), part of the Department for Science, Innovation and Technology ("**DSIT**"), collectively referred to as "**the parties**" throughout this document. References to the Commissioner include his statutory successors.
2. In particular, this MoU sets out the broad principles of collaboration and the legal framework governing joint working initiatives, and the sharing of relevant information and intelligence between the parties. The shared aims of this MoU are to enable closer working between the parties, including the exchange of appropriate information, so as to assist them in discharging their functions, and to avoid duplication of effort and unnecessary costs to public funds.
3. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the Commissioner or the CDEI. The parties have determined that they do not exchange sufficient quantities of personal data to warrant entering into a separate data sharing agreement, but this will be kept under review.

### Overall purpose

4. The purpose of this MoU is to set out the terms of the ongoing collaboration between the parties on matters relating to artificial intelligence and digital policy issues where their remits and interests intersect.
5. The parties are committed to fostering effective working relations, principally by promoting a culture of cooperation and collaboration between the two organisations and, when appropriate, meeting to discuss issues of common interest or concern.

## **The role and function of the Information Commissioner**

6. The Commissioner is a corporation sole appointed by His Majesty the King 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.
7. The Commissioner is empowered to take a range of regulatory actions for breaches of the following legislation:
  - Data Protection Act 2018 (DPA);
  - UK General Data Protection Regulation (UK GDPR);
  - Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR);
  - Freedom of Information Act 2000 (FOIA);
  - Environmental Information Regulations 2004 (EIR);
  - Environmental Protection Public Sector Information Regulations 2009 (INSPIRE Regulations);
  - Investigatory Powers Act 2016;
  - Re-use of Public Sector Information Regulations 2015;
  - Enterprise Act 2002;
  - Security of Network and Information Systems Directive (NIS Directive); and
  - Electronic Identification, Authentication and Trust Services Regulation (the "eIDAS").
8. Article 57 of the UK GDPR and section 115(2)(a) of the DPA 2018 place a broad range of statutory duties on the Commissioner, including monitoring and enforcement of the UK GDPR, 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 outlined in paragraph 7 above.
9. The Commissioner's regulatory and enforcement powers include:
  - conducting assessments of compliance with the DPA, UK GDPR, PECR, eIDAS, the NIS Directive, FOIA and EIR;

- issuing information notices requiring individuals, controllers or processors to provide information in relation to an investigation;
  - 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;
  - administering fines by way of penalty notices in the circumstances set out in section 155 of the DPA;
  - administering fixed penalties for failing to meet specific obligations (such as failing to pay the relevant fee to the Commissioner);
  - issuing decision notices detailing the outcome of an investigation under FOIA or EIR;
  - certifying contempt of court should an authority fail to comply with an information notice, decision notice or enforcement notice under FOIA or EIR; and
  - prosecuting criminal offences before the Courts.
10. 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 falls 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).

### **Functions and powers of the CDEI**

11. The CDEI is a government expert body enabling the trustworthy use of data and AI across the economy. It works in partnership with public sector organisations and industry bodies to develop, test and refine approaches to trustworthy data and AI governance, and addresses barriers to responsible innovation.

12. The CDEI is not a separate legal entity and operates as an Expert Directorate of DSIT. It is acknowledged that CDEI is therefore entering into MoU this as part of DSIT, and to the extent that it is necessary for the parties to enter into legally enforceable agreements for any reason, these shall be agreed and entered into by and between DSIT and the Commissioner.

### **Purpose of information sharing**

13. The purpose of the MoU is to enable the parties to work collaboratively in the areas specified above, which enhances their ability to exercise their respective functions.
14. This MoU should not be interpreted as imposing a requirement on either party to disclose information in circumstances where doing so would breach their statutory responsibilities or materially impact operational priorities. In particular, each party must ensure that any disclosure of personal data pursuant to these arrangements fully complies with the United Kingdom's General Data Protection Regulation (the "**UK GDPR**") and the Data Protection Act 2018 (the "**DPA 2018**"). The MoU sets out the potential legal basis for information sharing, but it is for each party to determine for themselves that any proposed disclosure is compliant with the law.

### **Principles of cooperation and sharing**

15. The parties recognise that they have a shared interest in promoting technological innovation for the public good which respects data privacy rights and ethical principles.
16. The parties intend to share information with each other, where they consider that such information sharing will help the other to effectively fulfil their respective functions. The parties acknowledge that the sharing of information will always be subject to compliance with applicable law. This may require, amongst other things, that they implement further information sharing arrangements before sharing sensitive personal data, or bulk quantities of personal data. If the parties do identify a need to enter into legal agreement(s) to govern the transfer of personal data, the Commissioner and DSIT will work together to identify and enter into appropriate legal terms.

17. The parties will endeavour to ensure timely and focussed exchange of relevant information that enables effective co-ordination and cooperation in the areas outlined in this MoU.
18. The Commissioner may offer provision of regulatory advice in the context of the CDEI's outputs, including projects, reports or guidance.
19. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at its discretion, the CDEI will alert the Commissioner to any potential breaches of legislation regulated by the Commissioner, that are discovered by the CDEI whilst undertaking its duties, and will provide relevant and necessary supporting information.
20. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at their discretion, the parties will:
  - a. Hold quarterly meetings at senior level to discuss matters of mutual interest;
  - b. Consult one another as appropriate on any issues or initiatives they are undertaking which might have significant implications for the other organisation;
  - c. Undertake to identify potential areas for joint working and make reasonable efforts to co-operate on these as appropriate; and,
  - d. Provide advice to each other as appropriate on issues relating to their respective functions and areas of interest.
21. The parties will comply with the laws they are subject to, including, but not limited to, local data protection laws. They will also maintain appropriate policies, procedures, and other internal governance requirements in order to support their compliance with applicable legal obligations.
22. The parties will exchange information on relevant issues of mutual interest, subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise), and as appropriate and relevant to their respective objectives. In doing so, the parties will work transparently and collaboratively, using their reasonable efforts to alert each other to issues which they

anticipate may have significant implications for the work of the other party.

## **Legal basis for sharing information**

### *Information shared by the CDEI with the Commissioner*

23. The Commissioner's statutory function relates to the legislation set out at paragraph 7, and this MoU governs information shared by the CDEI to assist the Commissioner in meeting those responsibilities. The CDEI must ensure, amongst other things, that its processing of personal data is compliant with the "data protection principles" and any other relevant requirements contained in the UK GDPR or DPA 2018.
24. Section 131 of the Data Protection Act 2018 may provide a legal basis for the CDEI to share information with the Commissioner. Under this provision, the CDEI is not prohibited or restricted from disclosing information to the Commissioner by any other enactment or rule of law provided it is "*information necessary for the discharge of the Commissioner's functions*".

### *Information shared by the Commissioner with the CDEI*

25. The Commissioner, during the course of his activities, will receive information, including personal data, from a range of sources. He will process all personal data in accordance with the UK GDPR, the DPA 2018 and all other applicable legislation. The Commissioner may identify that information he holds, which may include personal data, ought to be shared with the CDEI as it would assist them in performing their functions and responsibilities, in particular in areas of work generated by this MoU between the parties.
26. Section 132(1) of the DPA 2018 restricts the disclosure of information that (i) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, discharging his functions, (ii) relates to an identifiable individual or business, and (iii) is not otherwise available to the public from other sources. Such information may include, but is not limited to, personal data and may only be disclosed if the disclosure is made with lawful authority. Section 132(2) DPA 2018 provides that a disclosure of information falling within the scope of section 132(1) will be made

with lawful authority in a number of circumstances, in particular where the disclosure is:

- a. necessary for the purpose of the Commissioner discharging his functions (section 132(2)(c));
- b. made for the purposes of criminal or civil proceedings, however arising (section 132(2)(e)); or
- c. necessary in the public interest, having regard to the rights, freedoms and legitimate interests of any person (section 132(2)(f)).

27. The Commissioner will therefore be permitted to share information with the CDEI in circumstances where it has determined that it is reasonably necessary to do so in furtherance of one of those grounds set out under section 132(2) of the DPA 2018, and may do so where it will assist in the work referred to in this MOU. In doing so, the Commissioner will identify the function of the CDEI with which that information may assist, and assess whether that function could reasonably be achieved without access to the particular information in question. In particular, where the information proposed for sharing with the CDEI amounts to personal data the Commissioner will consider whether it is necessary to provide it in an identifiable form in order for the CDEI to perform its functions, or whether disclosing it in an anonymised form would suffice.
28. If information to be disclosed by the Commissioner was received by him in the course of discharging his functions as a designated enforcer under the Enterprise Act 2002, any disclosure will be made in accordance with the restrictions set out in Part 9 of that Act.
29. Where information is to be disclosed by either party for law enforcement purposes under section 35 (4) or (5) of the DPA 2018 then they will only do so in accordance with an appropriate policy document as outlined by section 42 of the DPA 2018.
30. Where a request for information is received by either party under data protection laws or the Freedom of Information Act 2000 ("**the FOIA**"), the recipient of the request will seek the views of the other party as described in the FOIA section 45 Code of Practice, where the information being sought under the request includes information obtained from, or shared by, the other party. However, the decision to disclose or withhold the information (and therefore any liability

arising out of that decision) remains with the party in receipt of the request as Data Controller in respect of that data.

### **Method of exchange**

31. Appropriate security measures shall be agreed to protect information shared between the parties in accordance with the sensitivity of the information and any classification that is applied by the sender.

### **Confidentiality and data breach reporting**

32. Where information that is subject to a duty of confidentiality is shared between the parties it will be marked with the appropriate security classification.
33. Where one party has received information from the other, it will, subject to applicable law, consult with the other party before passing the information to a third party or using the information in an enforcement proceeding or court case.
34. Where information held by one party (the originating party) that is subject to a duty of confidentiality has been provided to or shared with the other party (the receiving party), if the receiving party wrongfully discloses such information to a third party, the receiving party will bring the wrongful disclosure to the attention of the originating party without delay. This is in addition to any obligation to report a personal data breach under the UK GDPR and/or DPA 2018 where personal data is contained in the information disclosed.










### **Duration and review of the MoU**

35. The parties will monitor the operation of this MoU and will review it every two years.
36. Any minor changes to this memorandum identified between reviews may be agreed in writing between the parties.
37. Any issues arising in relation to this memorandum will be notified to the point of contact for each organisation.

### **Key contacts**

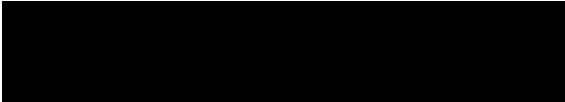
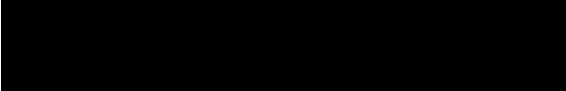
38. The parties have both identified a key person who is responsible for managing this MoU:



<b>Information Commissioner's Office</b>	<b>CDEI</b>
Sarah Meyers – Group Manager, Innovation Hub, ICO    	Emily Campbell-Ratcliffe – Head of AI Assurance, CDEI     

39. Those 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.

### Signatories

<b>Stephen Almond</b> Executive Director for Regulatory Risk, Information Commissioner's Office	<b>Felicity Burch</b> Executive Director, Centre for Data Ethics and Innovation
	
<b>Date:</b> 20 December 2023	<b>Date:</b> 22 December 2023

Note: This document has been signed and signatures redacted for publication.