

# Memorandum of Understanding between the Information Commissioner and the Surveillance Camera Commissioner

## Introduction

1. The Information Commissioner and the Surveillance Camera Commissioner have distinct responsibilities and interests for ensuring the effective regulation of surveillance cameras in the context of their own statutory roles. They are both committed to ensuring that there is close cooperation in the conduct of their respective statutory duties to ensure that there is effective regulation. In particular the Commissioners are committed to ensuring that regulatory activity is undertaken in a way which enables individuals, organisations and other stakeholders to be clear about how the responsibilities of the Commissioners are discharged individually, and collectively and also better understand their own responsibilities and rights in that regard.
2. This Memorandum of Understanding (MoU) establishes a framework for cooperation and information sharing between the Information Commissioner and the Surveillance Camera Commissioner, collectively referred to as "**the parties**" throughout this document. In particular, it sets out the broad principles of collaboration and the legal framework governing 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 regulatory functions.
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 Surveillance Camera Commissioner. 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.

## The role and function of the Information Commissioner

4. The Information Commissioner is a corporation sole appointed by Her Majesty the Queen 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.

5. The Information Commissioner is empowered to take a range of regulatory action for breaches of the following legislation:
  - Data Protection Act 2018 (DPA);
  - General Data Protection Regulation (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 (eIDAS).
6. Article 57 of the GDPR and Section 115(2)(a) of the DPA 2018 place a broad range of statutory duties on the Information Commissioner, including monitoring and enforcement of the 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 5 above.
7. The Information Commissioner's regulatory and enforcement powers include:
  - conducting assessments of compliance with the DPA, 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 Information 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.
8. 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 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 Surveillance Camera Commissioner**

9. The Surveillance Camera Commissioner is appointed by the Secretary of State for the Home Department under Section 34(1) of the Protection of Freedoms Act 2012 (PoFA).
10. PoFA applies to the use of overt surveillance camera systems (as defined by the Act) by relevant authorities in England and Wales.

Relevant authorities include Chief Officers of police, Police and Crime Commissioners and Local Authorities. Under the provisions of PoFA those organisations must have regard to the Secretary of State's Surveillance Camera Code of Practice (the Code) – failure to do so can be taken into account by any court of tribunal (s33.4, PoFA). The Code also requires the Surveillance Camera Commissioner to encourage voluntary adoption amongst all organisations and operators using surveillance camera systems.

11. The functions of the Surveillance Camera Commissioner include:
  - Encouraging compliance with the Code;
  - Reviewing the operation of the Code; and
  - Providing advice about the Code (including changes to it or breaches of it) and publish an annual report.
12. The Surveillance Camera Commissioner will provide information and advice on appropriate and approved ethical, operational and technical standards for various aspects of surveillance camera systems and on approved occupational and competency standards for persons using these systems or processing images and information obtained by these systems is expected to provide advice about the relevant operational, technical, quality management and occupational competency standards which are available for a system operator. In reviewing the operation of the Code the Surveillance Camera Commissioner considers the impact of this system of regulation against published success criteria and the opportunities to improve compliance in line with better regulation principles.
13. The Surveillance Camera Commissioner has produced a National Surveillance Camera Strategy (England and Wales). Implementation and oversight of this Strategy enables the Surveillance Camera Commissioner to more effectively discharge his statutory function in advising the Secretary of State as to the operation of the Code.

### **Purpose of information sharing**

14. The purpose of the MoU is to enable both the Information Commissioner and the Surveillance Camera Commissioner to share relevant information which enhances their ability to exercise their respective functions.

15. 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. In particular, each party must ensure that any disclosure of personal data pursuant to these arrangements fully complies with both the GDPR and the DPA 2018. The MoU sets out the potential legal framework 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**

16. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at their discretion, the Surveillance Camera Commissioner will alert the Information Commissioner to any potential breaches of the legislation regulated by her, within the context of this relationship, and within the scope of their statutory authority, discovered whilst undertaking regulatory duties, and provide relevant and necessary supporting information. Each party recognises that they should be mindful of the other's regulatory role, and will ensure that their own activities don't compromise the work of the other. This could, for example, apply to engagement with the media or other third parties.
17. Similarly, and again subject to any legal restrictions on the disclosure of information, the Information Commissioner will alert the Surveillance Camera Commissioner to any potential breaches of the Surveillance Camera Code of Practice within the context of this relationship and provide relevant and necessary supporting information.
18. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at their discretion, both parties will:
  - Communicate regularly to discuss matters of mutual interest (this may involve participating in multi-agency groups to address common issues and threats);
  - Consult one another on any issues which might have significant implications for the other organisation such as media announcements/coverage; and

- Engage regularly to consider opportunities for collaboration; this will be particularly relevant to projects that can streamline messaging and minimise regulatory confusion.
19. Both parties will comply with the general laws they are subject to, including, but not limited to, local data protection laws; the maintenance of any prescribed documentation and policies; and comply with any governance requirements in particular relating to security and retention, and process personal data in accordance with the statutory rights of individuals.

### **Lawful basis for sharing information**

#### *Information shared by the Surveillance Camera Commissioner with the Information Commissioner*

20. The Information Commissioner's statutory function relates to the legislation set out at paragraph 5, and this MoU governs information shared by the Surveillance Camera Commissioner to assist the Information Commissioner to meet those responsibilities. To the extent that any such shared information comprises personal data, as defined under the GDPR and DPA 2018, the Surveillance Camera Commissioner is a Controller so must ensure that it has a lawful basis to share it and that doing so would otherwise be compliant with the data protection principles. It must also ensure that sharing the information in question is consistent with its legal powers.
21. Section 131 of the Data Protection Act 2018 may provide both the lawful basis, from a data protection perspective, and the legal power for the Surveillance Camera Commissioner to share information with the Information Commissioner. Under this particular provision, the Surveillance Camera Commissioner is not prohibited or restricted from disclosing information to the Information 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 Information Commissioner with the Surveillance Camera Commissioner*

22. The Information Commissioner, during the course of her activities, will receive information from a range of sources, including personal data. She will process all personal data in accordance with the

principles of the GDPR, the DPA 2018 and all other applicable legislation. The Information Commissioner may identify that information she holds, which may include personal data, should be shared with the Surveillance Camera Commissioner, as it would assist him in performing his functions and responsibilities.

23. Section 132(1) of the DPA 2018 states that the Information Commissioner can only share confidential information with others if there is lawful authority to do so. In this context, the information will be considered confidential if has been obtained, or provided to, the Information Commissioner in the course of, or the purposes of, discharging her functions, relates to an identifiable individual or business, and is not otherwise available to the public from other sources. This therefore includes, but is not limited to, personal data. Section 132(2) of the DPA 2018 sets out the circumstances in which the Information Commissioner will have the lawful authority to share that personal data with the Surveillance Camera Commissioner. In particular, it will be lawful in circumstances where:

- The sharing was necessary for the purpose of the Information Commissioner discharging her functions (section 132(2)(c));
- The sharing was made for the purposes of criminal or civil proceedings, however arising (section 132(2)(e)); or
- The sharing was necessary in the public interest, taking into account the rights, freedoms and legitimate interests of any person (section 132(2)(f)).

24. The Information Commissioner will therefore be permitted to share information with the Surveillance Camera Commissioner in circumstances where it has been determined that it is reasonably necessary to do so in furtherance of one of those grounds outlined at paragraph 23. In doing so, the Information Commissioner will identify the function of the Surveillance Camera Commissioner 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 Surveillance Camera Commissioner amounts to personal data the Information Commissioner will



consider whether it is necessary to provide it in an identifiable form in order for the Surveillance Camera Commissioner to perform its functions, or whether disclosing it in an anonymised form would suffice.

25. If information to be disclosed by the Information Commissioner was received by her in the course of discharging her functions as a designated enforcer under the Enterprise Act 2002, any disclosure shall be made in accordance with the restrictions set out in Part 9 of that Act.
26. 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.
27. Where a request for information is received by either party under data protection laws, FOIA or EIR, and where the information being sought under that request includes information obtained from, or shared by, the other party, the recipient of the request will seek the views of the other party. In particular, the receiving party will have regard to the FOIA section 45 Code of Practice and/or the EIR regulation 16 Code of Practice as appropriate. 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, either as Controller in respect of that data or the public authority that holds the information under FOIA or EIR.

### **Method of exchange**

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

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

29. Where confidential material is shared between parties it will be marked with the appropriate security classification.
30. Where one party has received information from the other, it will consult with the other party before passing the information to a



third party or using the information in an enforcement proceeding or court case.

31. Where confidential material obtained from, or shared by, the originating party is wrongfully disclosed by the party holding the information, this party will bring this to the attention of the originating party without delay. This is in addition to obligations to report a personal data breach under the GDPR and/or DPA where personal data is contained in the information disclosed.

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

32. The Information Commissioner and the Surveillance Camera Commissioner will monitor the operation of this MoU and will review it biennially.
33. Any minor changes to this memorandum identified between reviews may be agreed in writing between the parties.
34. Any issues arising in relation to this memorandum will be notified to the point of contact for each organisation.

### **Designated Point of Contact**

35. Each Commissioner will identify a Designated Point of Contact (DPC) within their respective organisation who will be the primary point of contact with responsibility for communication between the two Commissioner bodies.
36. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) the key responsibilities of each DPC are as follows:
  - To ensure the effective and timely communication and receipt of information between the parties within the terms of this MoU;
  - To ensure that an appropriate assessment is made as to the relevancy and priority of any matter communicated so as to determine whether further action, dissemination of information or advice is appropriate and take responsibility for ensuring all areas of receipt and assessment of information of mutual

concern is effectively processed and that any such information is accompanied by clear decision making and effective dissemination;

- To horizon scan and identify potential areas of relevant interest and focus of each party which may overlap, duplicate effort, conflict or may otherwise benefit from a coordinated approach;
- To ensure that each Commissioner is notified promptly of any matter which is considered to merit their attention and this includes escalating matters to the Commissioners which are considered by either party to merit further action, or inaction, by one or both parties where agreement cannot be reached by the DPC's; and
- Maintain appropriate records of information which may assist the Commissioners in determining the effectiveness of the arrangements set out in this MoU. In particular the DPCs are responsible for identifying trends and areas where more strategic thinking or action may be of value on behalf of both parties.

**Key contacts**

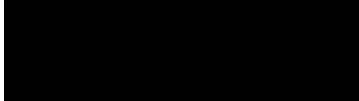
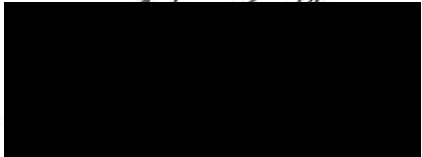
37. The parties have both identified a key person who is responsible for managing this MoU:

38.

<b>Information Commissioner's Office</b>	<b>The Surveillance Camera Commissioner's office</b>
<div style="background-color: black; width: 100%; height: 60px; margin-bottom: 5px;"></div> <p>Address: Wycliffe House, Water Lane, Wilmslow, SK9 5AF</p>	<div style="background-color: black; width: 100%; height: 60px; margin-bottom: 5px;"></div> <p>Address: 2 Marsham Street, 4<sup>th</sup> Floor Peel, London, SW1P 4DF</p>

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>Information Commissioner</b>	<b>Surveillance Camera Commissioner</b>
 Date: <i>Sept 18 / 2019</i>	 Date: <i>11 / 10 / 19</i>