Memorandum of Understanding between the National Crime Agency and the Information Commissioner

Introduction

1) This Memorandum of Understanding (MoU) establishes a framework for cooperation and information sharing between the National Crime Agency (NCA) and the Information Commissioner (the "Commissioner"), collectively referred to as "the Participants" 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 Participants.
2) The shared aims of this MoU are to codify and enhance working between the Participants, including the exchange of appropriate information, so as to assist them in discharging their functions. The MoU explains how the NCA and the Commissioner will work together in the following areas:
    a) Assessing and influencing improvements in cyber security of regulated organisations.
    b) Information sharing relating to entities subject to attack.
    c) Deconfliction between the NCA and the Commissioner in relation to incident management.
    d) Public communications and press releases.
3) This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the NCA or the Commissioner.

The Information Commissioner

4) The 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 Commissioner is empowered to take a range of regulatory action including for breaches of the following legislation:

- Data Protection Act 2018 (DPA 2018);
- 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;
- Network and Information Systems Regulations 2018 (the NIS Regulations); and
- Electronic Identification, Authentication and Trust Services Regulation (eIDAS).

6) 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 5) above.

7) The Commissioner's regulatory and enforcement powers include:

- conducting assessments of compliance with the DPA 2018, UK GDPR, PECR, eIDAS, NIS Regulations, 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 (as defined in section 3(9) of the DPA 2018) and other information rights obligations;
- administering fines by way of penalty notices in the circumstances set out in section 155 of the DPA 2018;
- 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.

8) 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).

The National Crime Agency

9) The National Crime Agency's (NCA) mission is to protect the public from serious and organised crime by targeting and pursuing those criminals who pose the greatest risk to the UK. We do this by:
   1) Degrading the most harmful organised crime groups that pose a threat to the UK;
   2) Leading the national operational response to serious and organised crime in the UK.

10) Section 1 of the Crime and Courts Act 2013 (CCA 2013) sets out the NCA's functions. These in particular include the NCA's crime reduction and criminal intelligence functions. The crime reduction function obliges the NCA to deal with both the quantity of activities undertaken to combat serious and organised crime; and the quality of such activities. The criminal intelligence function obliges the NCA to gather and disseminate information which is relevant to any kind of crime.

11) The Participants acknowledge the statutory power for the NCA to share data with the Commissioner pursuant to the working arrangements set out in this MoU will be section 7(4) of the CCA as the disclosure is for one or more of the permitted purposes in section 16(1) of the CCA, which includes for the exercise of any NCA functions.

12) The Participants acknowledge the statutory power for the ICO to share data with the NCA pursuant to the working arrangements set out in this MoU will be section 7(1) of the CCA as it will be in connection with the NCA's criminal intelligence and crime reduction functions.

13) The use of the information sharing gateway under section 7 of the CCA by the Participants will be subject to the statutory restrictions set out in schedule 7 to the CCA. In particular, the Participants recognise section 7 will not authorise a disclosure of personal data in contravention of data protection legislation.

14) The Participants acknowledge the proposed sharing of information for the "Agreed Purposes" (as set out in paragraph 20) will engage both Part 3 of the DPA 2018 ("law enforcement processing") and the UK GDPR / Part 2 Chapter 2 of the DPA 2018 ("general processing").

Assessing and influencing improvements in cyber security and cybercrime reporting

15) The NCA seeks to promote increased reporting of cybercrime in a manner that supports its work with regulators in the UK. Similarly, the Commissioner contributes to international standards and guidance through working with a range of regulatory partners across jurisdictions with the purpose of further international co-operation, including in relation to cyber security. The Commissioner and the NCA will inform each other about international developments and opportunities that would support their respective abilities to achieve these outcomes.

16) The Commissioner considers that a key part of the ICO's work is understanding what cyber security standards have been achieved in the organisations within its remit, what changes are most urgently needed, and how these changes can be implemented.

17) Through its guidance, the Commissioner will encourage good practice and continuous improvement in cyber security amongst the organisations it regulates. For example, the Commissioner's guidance will continue to promote engagement with the NCA via the reporting of cybercrimes, alongside other relevant good practice.

18) The National Cyber Strategy recognises the importance of working in partnership to successfully secure the UK in cyberspace. Consistent with this, the NCA seeks to promote positive cyber security cultures, and to foster learning from experience and peers. The Commissioner has regard to the value the National Cyber Strategy places on partnership and collaboration when exercising the statutory functions in relation to cyber security.

Information Sharing

19) For the avoidance of doubt, the NCA will not share information from an organisation it is engaged with due to a cyber incident with the Commissioner unless it has the consent of the organisation to do so.

20) The NCA and the Commissioner will share information to the extent permitted by law, and as appropriate and relevant to their respective missions, statutory functions and objectives ("Agreed Purposes"). The data will be shared via existing bespoke processes, such as the MAID meeting (Monthly Agency Incident Deconfliction) and email. Detail of data sharing may include, but is not limited to:

    a) The NCA sharing relevant cyber threat information with the Commissioner, including cyber threat assessments that are likely to affect Relevant Digital Service Providers (as defined under the NIS Regulations) and other organisations regulated by the Commissioner.

    b) The Commissioner sharing information about cyber incidents with the NCA (both on an anonymised, systemic and aggregated basis, and on an organisation-specific basis where appropriate) to assist the NCA's role in protecting the public from serious and organised crime.

21) Information that is directly or indirectly supplied to the Commissioner by, or that relates to, the NCA is exempt from Freedom of Information requests received by the Commissioner by virtue of Section 23 of the Freedom of Information Act 2000, and may be subject to exemption from disclosure under other information legislation. Any Freedom of Information requests made to the Commissioner for information that the NCA has supplied to the Commissioner should be referred to the NCA.

22) The Participants understand that once they are in receipt of the information, they will be a data controller for that data and will be responsible for complying with the principles of the DPA 2018 in relation to its further processing of that data.

23) The Commissioner will not make any onward disclosure of data shared by the NCA, except with the prior consent of the NCA.

Subject Rights Requests

24) The Participants will answer any subject access or other rights requests that they receive which relate to the processing they are undertaking whilst they are still processing the information received under this MoU. The receiving Participant will provide the sending Participant with reasonable assistance in complying with any Data Subject rights requests it may receive in relation to its processing of the information received under this MoU.

25) The receiving Participant will not disclose or release any information received under this MoU in response to a Data Subject access request, without first consulting the sending Participant, wherever possible.

Method of exchange

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

27) For example, where information being shared by the NCA is classified as secret or above, or is particularly sensitive, or is otherwise marked for limited distribution (e.g. by use of the traffic light protocol or otherwise), the NCA and the Commissioner will agree safeguards are put in place and maintained. This may include limiting distribution within the Information Commissioner's Office to named individuals or those with appropriate security clearance, if required.

Deconfliction between the NCA and the Commissioner in relation to incident management

28) Where organisations report an incident to the NCA and the NCA identifies that the case may be legally reportable to Commissioner, the NCA will remind organisations to be mindful of their regulatory obligations, but will not opine on whether an organisation may be under an obligation to notify nor make notifications to the Commissioner on the organisation's behalf.

29) Where organisations have notified the Commissioner of a cyber incident and it is identified through engagement with the affected organisation that the case may be relevant to the work of the NCA, the Commissioner will recommend and encourage the organisation to notify the NCA.

30) When both Participants are engaged in managing a cyber incident, the Participants will seek to co-ordinate their work to the extent reasonably

practicable and appropriate to minimise any disruption of the affected organisation's efforts to contain and mitigate any harm.

31) The NCA and the Commissioner recognise that the priority for an organisation suffering an incident should be the incident's remediation and the mitigation of harm to the organisation, its customers, and the UK and its citizens more generally. Both Participants will seek to ensure that their interventions align with this priority and will provide each other with feedback where they view the other's approach to intervention may have worked against it.

32) The Commissioner acknowledges that cross government coordination in response to an incident is required. Should the Commissioner intend to issue public communications concerning an incident, it will seek to ensure that where relevant it shares such communications with NCA in advance.

Public communications and press releases

33) Public communications on matters involving both Participants will, as far as is reasonably practicable, be agreed between the Commissioner and the NCA in advance, to support consistency. Where appropriate and relevant, the NCA and the Commissioner will also consult with their respective partner agencies and bodies.

34) Where appropriate, the Commissioner and NCA will seek to amplify each other's messages and an awareness of their differing interests; promote learning, consistent guidance and standards as well as key messages on information and cyber related matters.

35) All communications, whether related to a specific incident or more generally, will be mindful of the need to set out the distinct roles of the Commissioner and the NCA.

Management of the MoU

36) Under this MOU, the Participants will work constructively with each other. To support this, the Participants will provide feedback from time to time on the quality of the working relationship between them and, as necessary, consider changing how they engage with each other to achieve an effective working relationship. The Participants have both identified a key person who is responsible for managing this MoU:

37) Persons responsible:

Information Commissioner's Office	National Crime Agency
Stephen BONNER Deputy Commissioner, Regulatory Supervision Information Commissioner's Office Email: stephen.bonner@ico.org.uk Address: Wycliffe House, Water Lane, Wilmslow SK9 5AF	Paul FOSTER Deputy Director National Crime Agency National Cybercrime Unit Email: paul.foster3@nca.gov.uk Address: Citadel Place, Tinworth Street, London SE11 5EF

38) These 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.

39) The Participants will monitor the operation of this MoU and will review it every two years.

40) Any minor changes to this MoU identified between reviews may be decided in writing between the Participants.

41) Any issues arising in relation to this memorandum will be notified to the point of contact for each organisation (as identified above).

42) The NCA and ICO will both uphold and respect this MoU.

Signatories

Stephen BONNER Deputy Commissioner, Regulatory Supervision Information Commissioner's Office	James BABBAGE Director General - Threats National Crime Agency
Date: 05/09/2024	Date: 05/09/2024