MEMORANDUM OF UNDERSTANDING
Information Commissioner's Office and the UK Intelligence Community

Introduction

1. This Memorandum of Understanding (MOU) between the Secretary of State for the Home Department, the Secretary of State for Foreign and Commonwealth Affairs and the Information Commissioner, establishes a framework for co-operation between the United Kingdom Intelligence Community (UKIC) (MI5, SIS and GCHQ – "UKIC Agencies") and the Information Commissioner's Office (ICO), regarding responsibilities under the Data Protection Act 2018 (DPA).

2. Specifically, this MOU provides guidelines for the co-operation between UKIC Agencies and the ICO in the operation of Part Four of the DPA, "Intelligence Services Processing".

3. This MOU replaces, with reference to the UKIC Agencies, the previous Data Protection MOU that was signed by the Right Honourable Chris Grayling MP, the then Secretary of State for Justice and Christopher Graham, the then Information Commissioner, in September and July 2013 respectively.

Legal Status

4. This MOU is not intended to be legally binding and does not create legal rights or obligations between the signatories.

Purpose

5. The purpose of this MOU is to ensure consistent and good standards of co-operation between the UKIC Agencies and the ICO, in cases where:

a. Notification of a serious personal data breach is required in accordance with section 108 of the DPA;

b. A UKIC related data subject complaint has been received by the ICO.

6. This MOU takes effect subject to the DPA and any other relevant legal provisions, and should be read alongside any relevant ICO guidance or Codes of Practice. For the avoidance of doubt, nothing in this MOU will operate to restrict or otherwise inhibit the exercising of the powers and duties of the ICO.

Engagement with the ICO

7. Routine engagement between the ICO and the UKIC Agencies will be between the relevant Agency Data Protection Team, led by the respective Data Protection Officer (DPO), and the ICO Intelligence and High Priority Investigations or Investigations Directorates. Messages and material will be passed using appropriately classified systems to facilitate such communication.

8. It is recognised that national security cases will normally be particularly sensitive and it is accepted that the sensitivity of such cases means that there will often be a need for greater dialogue between the Information Commissioner and UKIC Agencies before the Commissioner reaches any final conclusions.

Notification of Serious Personal Data Breaches

9. Section 108 of the DPA stipulates the UKIC Agencies' duty to report serious personal data breaches to the ICO (subject to any national security exemptions, and the exception in section 108(6) for compliance errors under the IPA which are reportable to IPCO). See **ANNEX A** of this MOU for the UKIC guidance of what factors should be considered when determining whether a serious personal data breach has occurred.

Notification Process

10. When a personal data breach occurs, which the reporting UKIC Agency has assessed to meet the threshold of seriousness to require reporting to the ICO, the DPO of that UKIC Agency will contact a senior member of staff with appropriate Developed Vetting clearance at the ICO as soon as practicable to notify them of the breach. This contact will meet the notification requirement for a serious personal data breach to be ordinarily reported to the ICO within 72 hours as per section 108(2) of the DPA. Given the sensitive nature of the work undertaken by UKIC Agencies, it will not always be possible for this initial notification to include all the information set out at section 108(3) of the DPA, however, where it has not been possible to provide this information initially further details on the breach will follow without undue further delay (using more secure ways to share information if needed).

11. Given the complexities of UKIC Agency internal investigations and governance processes, it is understood and agreed that there may be occasions where it may not be possible to make this initial contact within the 72-hour timeline whilst facts are still being ascertained. In such instances, the reporting UKIC Agency will provide the ICO with an explanation for the delay. Where it is not possible to provide all the information required in the initial contact, the information will be provided in phases as soon as possible, meeting the obligations set out at section 108(4) of the DPA.

Follow on Actions

12. Following the initial contact, and subsequent discussion, the UKIC Agency DPO and the ICO contact will agree a process, timeframe and recording method for keeping the ICO apprised of the breach and subsequent investigation. That process will include, where possible, the provision of information sufficient to enable the ICO to conduct its own investigation in accordance with its statutory obligations.

13. Consideration should be given, where possible at this stage as to whether the response to the ICO can be provided within 20 working days as set out in para 17 below. If UKIC are unable to provide a response to the ICO within 20 working days, a proposed timescale should be provided if possible, to enable the ICO to respond to any query that may be received from a data subject whose data may have been breached.

Investigation Conclusion

14. When the UKIC Agency considers it has concluded its breach investigation, it will report its conclusions to the ICO, providing as much information as is appropriate.

15. It is recognised that, in order to discharge its important regulatory functions, the ICO will expect relevant information about the breach to satisfy the Commissioner and enable them to understand the nature and seriousness of the breach and to ensure that it can comply with its statutory obligations which may include regulatory and enforcement action as set out in parts 5 and 6 of the Act respectively.

Data Subject Complaints

16. Upon the ICO receiving a complaint from a data subject, the ICO will want to satisfy themselves that the issue has been handled correctly, and, where applicable, that the application of any exemption has been used appropriately. In doing so they will pay due regard to any exemptions that may be applicable, including the national security exemption, and the contents of any national security certificate issued by a Secretary of State under section 111 of the DPA.

17. Should ICO caseworkers request an explanation for the response made by a UKIC Agency, the response will be provided to the ICO within 20 working days. Where the UKIC Agency requires this to be classified as SECRET or above it will need to be appropriately secured at the ICO premises, or stored on the ICO's behalf at UKIC premises. The classification of the response will depend on the circumstances of each case and where appropriate will include a general description of the searches carried out and whether the national security exemption has been relied upon (whether by a Neither Confirm Nor Deny (NCND) response or refusal). If personal data is held, where applicable, the UKIC Agencies will state in broad terms why any exemption has been applied and why the material cannot be released (for example it relates to a covert investigation or operation, or it would impair UKIC operations). If an NCND response is given then a similar statement describing why this is necessary will be provided.

18. If the matter is particularly sensitive, the ICO will ensure the Case is transferred to a senior ICO member of staff with appropriate Developed Vetting clearance, and that all further communications are made through secure means, if available. Alternatively, the ICO will be briefed at UKIC Agency premises.

19. The UKIC Agency response will be held securely and in confidence by the ICO, and not communicated to the data subject. If the UKIC Agency relies on an NCND response, and the ICO is satisfied with this approach, the ICO will not reveal to the data subject whether personal data is held.

Requests for Information to the ICO

20. The ICO will undertake to engage with the relevant UKIC Agency in relation to any relevant Subject Access Requests they may receive, and the ICO will give due consideration to any representations received.

National Security Certificates

21. Under section 130(1) of the DPA a copy of the Certificate signed by a Minister of the Crown must be sent to the Commissioner and section 130(2)-(5) sets out the obligations of the ICO in respect of any such certificate which includes publishing a record of the certificate and, subject to subsection 130(4) the text of the certificate.

Term and Review

22. This MOU:

a. Will only be varied by written agreement between the signatories.

b. Will be reviewed formally every three years, and otherwise if requested by the signatories.

SIGNATORIES:

Signed by: Secretary of State for the Home Department

Signature: [redacted]

Name: Rt Hon Priti Patel

Date: 28/02/20

Signed by: Secretary of State for Foreign and Commonwealth Affairs

Signature: [redacted]

Name: Rt Hon Dominic Raab

Date: 26/2/2020

Signed by: Information Commissioner

Signature: [redacted]

Name: Elizabeth Denham

Date: 12/3/2020

ANNEX A – UKIC Guidance on Serious Personal Data Breaches

1. In section 84(4) of the Data Protection Act (DPA) a 'Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed'.

2. Section 108 of the **Data Protection Act** provides that, if a data controller becomes aware of a serious personal data breach in relation to personal data for which the controller is responsible, the controller must notify the Information Commissioner of the breach without undue delay.

3. By virtue of section 108(6), data breaches which are 'relevant errors' for the purposes of section 231(9) of the **Investigatory Powers Act 2016** are excluded from the scope of the notification obligation. This falls within the remit of the Investigatory Powers Commissioner.

4. Section 108(7) provides that for these purposes a breach is serious if it seriously interferes with the rights and freedoms of the data subject.

5. In considering whether the 'serious breach' threshold has been reached, it is suggested that all the facts and circumstances of the breach should be taken into account. This will include the following factors:

(a) The likely **severity of the impact** of the breach on the rights and freedoms of the data subject, i.e. how much harm, prejudice or damage is likely to be caused to those rights;

(b) The **scale** of the data breach, whether it involves just one data subject or hundreds/ thousands;

(c) The **extent of the interference with the right to privacy** under **Article 8/ECHR**, in the sense of the number of people to whom the data subject's personal data has been exposed or potentially exposed, e.g. in the case of a data loss, whether the data loss occurred externally or internally;

(d) Whether the data breach involves personal data that falls within one of the **'sensitive categories'** (i.e. one of the six categories of personal data listed in the definition of '**sensitive processing**' in Section 86(7)); and

(e) The **nature of the rights and freedoms of the data subject which have been impacted** – e.g. a loss of data which potentially jeopardised a data subject's right to life under **Article 2/ECHR** would be regarded as particularly serious.