# NATIONAL CRIME AGENCY

OPERATING PROCEDURE: NCA Bulk Personal Datasets
Reference: IM01 OP08 (v9.0)

---

## 1. Introduction

This Operating Procedure sets out the National Crime Agency (NCA) processes for managing "Bulk Personal Datasets" ("BPDs") throughout their lifecycle.

In doing so it prescribes the arrangements which apply to NCA officers[1] for the acquisition, retention, examination, disclosure and destruction of BPDs and specifies when an authorisation is required. The Operating Procedure requires consideration of the necessity and proportionality for processing BPDs, and ensures sufficient safeguards are in place throughout the BPD lifecycle.

The management of BPD was put on a statutory footing for the UK Intelligence Community ("UKIC") in Part 7 of the Investigatory Powers Act 2016 ("the IPA"). In setting out procedures for the NCA, this Operating Procedure takes into account the requirements of Part 7 of the IPA and the supplementary Code of Practice[2] ("the Code"). In interpreting the requirements of this Operating Procedure, reference should be made to the further detail contained in the Code.

The NCA identifies and reviews all BPDs it currently retains to ensure compliance with this Operating Procedure.

The NCA recognises that the laws and principles in relation to the processing of BPDs are evolving and subject to change. Accordingly, the NCA will continue to keep this Operating Procedure under regular review.

This Operating Procedure supports and supplements the NCA's published Information Charter.

[1] "NCA Officers" has the meaning ascribed to it in section 16 of the Crime and Courts Act 2013– see Annex A.
[2] Intelligence services' retention and use of bulk personal datasets Code of Practice published pursuant to Schedule 7 to the IPA 2016 (March 2018).

## 2. Key Points

- All BPDs held by the NCA are subject to the 'six-step' test (see Para 3.2) to identify whether a BPD authorisation is required to retain, select data for examination and/or disclose the dataset.

- Following any permitted 'initial examination' period an application must be submitted to the relevant issuing authority (the NCA Data Authorisation Panel (sitting as part of the Data Governance Board) for authorisation. Once authorised, these will be valid for a period of up to 12 months, and must either be renewed or cancelled at the end of this period. Regular reviews will be undertaken to ensure justification for authorisation is on-going.

- All applications for authorisation must be on the relevant form (IM01 F02 – BPD Initial Application Form) and justify the necessity and proportionality for the proposed activity and identify sufficient safeguards for management of the dataset throughout its lifecycle. BPDs must be destroyed, once an authorisation is cancelled or when an authorisation is refused.

- NCA compliance with this Operating Procedure is overseen by the Information Commissioner (ICO).

## Part 1: BPD in the NCA

## 3. Requirements

3.1 The NCA needs to obtain a range of information from a variety of sources in connection with the exercise of its functions. NCA functions include both a crime reduction function and a criminal intelligence function under the Crime and Courts Act 2013 (CCA).

3.2 Among the range of information obtained are BPDs. A dataset which has been obtained, or that will be obtained, by the NCA in the exercise of its functions comprises a BPD where:

- *the data relates to a number of individuals;*

- *the data comprises personal data – for these purposes, 'personal data' has the same meaning as in the Data Protection Act 2018[3] (DPA), except that it also includes data relating to a deceased individual where the data would be personal data if it related to a living individual;*

[3] Section 3 (2) of the Data Protection Act 2018 defines personal data as "any information relating to identified or an identifiable living individual". This means an individual who can be identified, directly or indirectly, in particular with reference to; (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

- *the Director General of the NCA is, or will be, the data controller[4];*
- *the NCA intends to retain, examine and/or disclose the dataset for the exercise of its functions (after any initial examination of the contents);*
- *the majority of individuals are not, and are unlikely to become, of interest to the NCA in the exercise of the function (or functions) for which the dataset is retained, examined and/or disclosed – where a dataset is retained and examined for a specific function and the majority of individuals are of interest to the NCA, the dataset will not constitute a BPD;*
- *the data is held, or is to be held, electronically for analysis in a form capable of selection for examination[5] by NCA officers in the exercise of the NCA's functions.*

3.3 BPDs may be acquired through overt or covert means. BPDs will provide information about individuals of interest to the NCA but will also include information about individuals who are of no direct relevance to the NCA in the exercise of its functions. In the case of BPDs it is not practicable to acquire the information that will be of direct value to the NCA without also acquiring this additional data; indeed, at the point of acquisition it may not be known exactly which information will prove to be of value.

3.4 The NCA draws on BPDs and uses selected data in conjunction with other data in order to exercise its functions. This includes using the data to facilitate the exclusion of individuals from an investigation and to ensure that the activities of the NCA are correctly focused on those individuals or organisations that are relevant to the exercise of its functions.

3.5 The acquisition, retention, examination and disclosure of BPDs requires both operational and legal justification (including necessity and proportionality), accompanied by detailed and comprehensive safeguards against misuse. Once retention cannot be justified on those grounds any longer, the dataset must be destroyed.

3.6 For the avoidance of doubt, this Operating Procedure applies to BPDs obtained under the NCA's information gateway in section 7 of the CCA and gateways in other legislation[6].

[4] The DG of the NCA will be the data controller where the NCA determines the purposes for which and the manner in which any personal data are, or are to be, processed. Accordingly, datasets being processed by third parties (as a data processor) on behalf of the NCA can amount to BPD as the DG NCA is the data controller.

[5] For the purposes of this Operating Procedure, the selection of data includes the:
(1) organisation, adaptation or alteration of data from the BPD;
(2) retrieval, consultation or use of data from the BPD; and
(3) alignment or combination of data from the BPD with other information or datasets.

Data retained and examined for primary and secondary purposes

3.7 BPD authorisation is not required if all of the following provisions apply:

a) the data has been acquired under one of the statutory powers set out in the exhaustive list[7] entitled 'Commonly Used Powers (for retention, exploitation and disclosure of information)' at Annex E, and at paragraph 3.11, and;

b) the NCA must (or has the power to) retain and use the data in the manner provided for by the statutory functions on the list at Annex C and a time limit on retention of data by the NCA has been set to ensure compliance with that power, and any other applicable statutory requirements, and;

c) the NCA is retaining, examining and/or disclosing the data only pursuant to that power(s) and no other.

3.8 Where NCA officers have acquired a dataset in the manner outlined at 3.7(a) above but, in the course of events, it becomes necessary for NCA officers to retain/examine/disclose it for any other purpose, the dataset should fall for consideration under the BPD authorisation process in the normal way[8]. This includes any requirement by an NCA officer to:

a) hold the data for any longer than governed by the primary[9] purpose, and/or;

b) disclose the data for any reason other than that governed by the primary purpose, and/or;

c) use (i.e. retain/examine) the data in any way differently, or outside of, the purpose for which it was initially acquired, retained or examined.

3.9 For clarity, it is recognised that a consequence of this process may be that the same dataset will be held concurrently by the NCA subject to two statutory bases; both the original (primary) statutory basis under a Commonly Used

[6] For example, UKIC may disclose information to the NCA in accordance with intelligence service disclosure arrangements.
[7] The list may be extended if there is a legitimate basis for doing so. Referrals should be made to CDO who will seek the concurrence of the NCA Legal team.
[8] Note that it is still possible that the dataset is assessed to fall outside the legal definition of a BPD – e.g. if the majority of individuals are assessed to be of interest to the NCA – but the applicant officer still needs to go through the process and in particular, to complete Section 2 of the BPD application form to determine whether or not the dataset is, in fact, a BPD
[9] Primary means the first purpose, and does not mean the main purpose.

Power on the list in Annex E and on a secondary basis, authorised under the BPD process in order to permit examination/disclosure by NCA officers in furtherance of the exercise of their powers pursuant to alternative statutory functions[10].

3.10 Where NCA officers propose to process data from seized devices for a secondary purpose, this may be authorised under an Overarching Seized Device Data BPD Authorisation detailed at paragraph 6.9 – 6.12.

Authorisations under the Investigatory Powers Act 2016

3.11 Subject to 3.12 below, if a dataset (that would otherwise meet the legal definition of a BPD) has been acquired under the IPA, a BPD authorisation is not required and will be governed by the applicable regime under the relevant part of the Act[11].

3.12 After retaining a dataset acquired under the IPA for a period of 6 months, the NCA must delete it, unless (in circumstances where NCA officers wish to continue to retain, examine and/or disclose the dataset), NCA officers either:

a) follow the BPD authorisation process[12], or

b) identify a statutory requirement/legal basis from the exhaustive list entitled 'Commonly Used Powers (for retention, exploitation and disclosure of information)'[13] at Annex E under which the NCA is permitted to retain, examine and/or disclose the dataset. NCA officers must be satisfied that the dataset is being held for that purpose and that purpose only, in which case, the NCA may continue to hold it for that purpose, without seeking a BPD authorisation. If the dataset is wanted for any other use or purpose, or it has been retained/examined under a statutory power not on the exhaustive list, the dataset must be considered for BPD authorisation or deleted.

[10] The CCA makes provision for the NCA and its various powers and functions.
[11] Section 201 IPA 2016: "*Section 200 (1) or (2) does not apply to the exercise of a power of an intelligence service to retain or (as the case may be) examine a bulk personal dataset if the intelligence service obtained the bulk personal dataset under a warrant or other authorisation issued or given under this Act*". Section 200 (1) and (2) govern the general requirement for authorisation by a warrant to retain/examine BPDs.
[12] Note – it is still possible that the dataset, initially acquired under the IPA 2016, is assessed to fall outside the legal definition of a BPD – e.g. if the majority of individuals are assessed to be of interest to the NCA. Nevertheless, the applicant officer must still go through the process and in particular, complete Section 2 of the BPD application form to determine whether or not the data is, in fact, a BPD.
[13] For example, Proceeds of Crime Act 2002, Police and Criminal Evidence Act 1984.

## 4. The Law

### 4.1 *The Crime and Courts Act 2013*

The CCA sets out the functions of the NCA and provides a statutory information gateway.

### 4.2 *The data protection legislation includes the GDPR and the Data Protection Act 2018 ("the data protection legislation[14]")*

The Director General of the NCA is the data controller for all personal data held by the NCA. Accordingly, when NCA officers process any BPDs, they must ensure that they comply with the provisions of the Data Protection Legislation.

### 4.3 *The Human Rights Act 1998 ("the HRA")*

The NCA is a public authority for the purposes of the HRA. When acquiring, retaining, examining and disclosing BPDs, the NCA must (among other things) ensure that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights ("ECHR"). In practice, this means that any interference with privacy must be in accordance with the law, necessary for the performance of its function and proportionate to the achievement of that objective. Other rights may also be engaged, such as the right to freedom of expression (Article 10).

### 4.4 *The Criminal Procedure and Investigations Act 1996 ("the CPIA")*

Where a BPD has been obtained in the course of a criminal investigation and it may be relevant to that investigation, it must be retained in accordance with CPIA and established disclosure requirements.

## 5. Governance

5.1 The Data Authorisation Panel ("DAP") sitting as part of the Data Governance Board ("DGB") oversees NCA officers' compliance with this Operating Procedure. It maintains records of decisions and a schedule of BPDs is maintained within the NCA Master BPD Schedule.

5.2 Voting membership of the DAP is restricted to Deputy Director level. A minimum attendance of two voting members plus Legal's representative is required for decisions, with the relevant Information Asset Owner ("IAO") excluded from voting in individual cases.

[14] See section 3(9) DPA 2018.

## 6. Authorisation

6.1 Save as set out at paragraph 3.11 of this Operating Procedure, authorisation must be obtained for (a) the retention of all BPDs, (b) the selection of data from a retained BPD for examination (a "BPD Authorisation"), (c) the retention of Class BPD Authorisations and (d) the retention of BPDs from seized devices under Overarching Seized Device Data Authorisations. An authorisation must also be obtained for the disclosure of any BPDs to persons outside of the NCA (BPD Disclosure Authorisation IM01 F30).

6.2 Prior to obtaining a dataset, NCA officers should consider (based on the information available at the time) whether a BPD Authorisation will be required for the retention and examination of that dataset.

6.3 A BPD Authorisation should be sought as soon as it is apparent that: (1) the dataset is a BPD or (2) that there is a Class Authorisation which contains protected data or health records that require a specific authorisation and (3) that BPD is of a nature that the NCA would wish to (a) retain it, (b) select data for examination from it and/or (c) disclose it.

*Types of BPD Authorisation*

6.4 Three types of BPD Authorisation can be applied for:

- 'Specific BPD Authorisation' authorising NCA officers to retain and select data for examination from the particular BPD described in the authorisation, and;
- 'Class BPD Authorisation' authorising NCA officers to retain and select data for examination from BPDs that fall within a class described in the authorisation, and;
- 'Overarching Seized Device Data BPD Authorisation' authorising NCA officers to retain and select data for examination from BPDs arising from seized devices which are processed for a secondary purpose.

6.5 A Class BPD Authorisation is for BPDs which are (a) similar in their content and proposed use, and (b) raise similar considerations as to necessity and proportionality, including the intrusiveness of the data.

6.6 A Class BPD Authorisation cannot be issued if:

- the BPD consists of, or includes, protected data;
- the BPD consists of, or includes, health records;
- a substantial proportion of the BPD consists of personal data the processing of which would be sensitive processing within the meaning of that term in s35 (8) of the Data Protection Act 2018 (DPA).

or;

- the nature of the BPD, or the circumstances in which it was created, is such that its retention or examination raises novel or contentious issues which ought to be considered by a Specific BPD Authorisation.

6.7 In these circumstances, a Specific BPD Authorisation (see 6.8 below) will be required. Additional guidance is provided at Annex B.

6.8 A Specific BPD Authorisation can also authorise the retention of and selection of data for examination from replacement datasets. For the purposes of this Operating Procedure, a replacement dataset is a dataset that does not exist at the time the Specific BPD Authorisation is issued, but may reasonably be regarded as a replacement for the BPD specified in that authorisation. Where the retention of a replacement dataset or selection of data for examination from a replacement dataset is to be permitted, this must be expressly stated in the Specific BPD Authorisation.

*Overarching Seized Device Data BPD Authorisations*

6.9 An Overarching Seized Device Data BPD Authorisation is for BPDs which arise from seized devices that are to be processed for a secondary purpose.

6.10 An Overarching Seized Device Data BPD Authorisation can only authorise the use of BPDs for a secondary purpose if they have arisen from devices that have been lawfully obtained or lawfully seized under one of the Commonly Used Powers listed at Annex E or obtained from partners.

6.11 Once an NCA officer has obtained an Overarching Seized Device Data BPD Authorisation, they are required to make a 'Specific Request to Process Bulk Personal Data from Seized Digital Devices' via form IM01 F60 each time BPDs from a new device or group of devices are to be acquired to ensure prior authorisation to process the BPDs.

6.12 The 'Specific Request to Process Bulk Personal Data from Seized Digital Devices' will be considered at the CDO, Legal and NDEC (CLaN) meeting for approval. A Grade 2 from Legal and CDO must be present to approve a 'Specific Request to Process Bulk Personal Data from Seized Digital Devices'.

*Applications*

6.13 When completing an application, NCA officers must ensure that the case for authorisation is presented in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for authorisation.

6.14 All applications must be read and endorsed by an Accountable Business Area Manager (ABAM).

6.15 The DAP can issue (a) Specific BPD Authorisations, (b) BPD Disclosure Authorisations, (c) Class BPD Authorisations, (d) Overarching Seized Device Data BPD Authorisation in accordance with its terms of reference.

6.16 The DAP has the authority to issue Specific BPD Authorisations, BPD Disclosure Authorisations, Class BPD Authorisations and Overarching Seized Device Data BPD Authorisation. All BPD authorisations including Class BPD Authorisations will be presented for noting and enquiry at by the Data Governance Board ("DGB").

6.17 For the purposes of this Operating Procedure, the body which determines whether to issue an authority, will be referred to as the "Issuing Authority".

6.18 All authorisations are addressed to a named Accountable Business Area Manager (ABAM) who is accountable for overseeing compliance with this Operating Procedure.

6.19 If an application for authorisation is refused, the Issuing Authority will provide a written explanation for its decision to the applicant including any conditions permitting further application.

*Duration*

6.20 Authorisations last for up to 12 months from the date of issuance. After this date and unless the authorisation is renewed, the authorisation will cease to have effect and the dataset must be destroyed. A cancellation (form IM01 F04) should be submitted, as soon as retention of the BPD no longer satisfies the grounds for authorisation.

*Review*

6.21 ABAMs must review on an on-going basis the operational and legal justification for the continued retention and examination of each BPD. Any significant changes that influence the basis on which the authorisation was granted must be brought to the attention of the relevant Issuing Authority at the earliest opportunity.

*Renewals*

6.22 An authorisation may be renewed by application to the Issuing Authority (form IM01 F03 – including an endorsement by the ABAM). Applications for renewal should be made prior to the expiry of the existing authorisation but should normally only be renewed in the last 30 working days of the period for which

the authorisation has effect. If renewal is authorised by the Issuing Authority, the renewed authority will be issued to the ABAM.

6.23 A Class BPD Authorisation may be renewed by application via form IM01 F03 to the Issuing Authority. The renewal application must list any new BPDs added to the class, including rationale for the new BPDs meeting the criteria of the class.

6.24 An Overarching Seized Device Data BPD Authorisation may be renewed by application via form IM01 FXX to the Issuing Authority. The renewal application must list any new BPDs added via Specific Request since the previous authorisation.

*Modifications*

6.25 An authorisation may be modified by an application to the Issuing Authority (form IM01 F02 – including an endorsement by the ABAM) or at the Issuing Authority's own direction. If modifications are authorised, the Issuing Authority will issue a new modified authority to the ABAM.

6.26 Modifications can only add, vary or remove any operational purpose specified in the authorisation.

*Cancellations*

6.27 The Issuing Authority may cancel an authorisation at any time. If any NCA officer (including the applicant or ABAM) considers that an authorisation no longer satisfies the grounds for authorisation (including necessity and proportionality), the Issuing Authority must be informed and cancellation of the authorisation must be sought (form IM01 F04 – including an endorsement by the ABAM). The Issuing Authority will issue the cancellation which will be addressed and communicated to the ABAM.

*Urgent processes*

6.28 Urgent applications or modifications can only be made for a Specific BPD Authorisation or BPD Disclosure Authorisation. It is not possible to seek an urgent application or modification for a Class BPD Authorisation or Overarching Seized Device Data BPD Authorisation.

6.29 A member of the relevant Issuing Authority can urgently authorise the retention, selection for examination or disclosure of a BPD, if that individual believes that (a) the grounds for the authorisation have been satisfied; and (b) the urgency criteria below are met.

6.30 Urgent authorisations may only be made if it would not be reasonably practicable to obtain approval from two quorate members plus Legal

representative of the relevant Issuing Authority in the time available and it is necessary to retain, select data for examination or disclose a BPD urgently because there is:

- An imminent threat to life or serious harm;
- A significant investigative opportunity; or
- A significant intelligence-led opportunity, which is significant because of the nature of the potential intelligence or because the operational need for the intelligence is significant, and the opportunity is rare or fleeting.

6.31 The DAP Chair and one additional DD from the DG Operations command can urgently authorise the retention, examination or disclosure of a BPD (excluding Class BPD and Overarching Device Data BPD). This is in accordance with the provisions set out in sections 6.29 - 6.31 of the BPD Operating Procedure.

6.32 All urgent authorisations and modifications must be reviewed by a quorate DAP as soon as practicable. The Operational DD/IAO or delegate DAP Chair should not have a conflict of interest with urgent BPD Authorisation(s).

## 7. External Oversight

7.1 Compliance with the data protection legislation in relation to processing bulk personal data under this Operating Procedure including in relation to the authorisation, use, retention and disclosure of bulk personal datasets by the NCA, and the management controls and safeguards against misuse put in place, will be overseen by the ICO as regulator for that legislation. The ICO also has general oversight of the NCA's compliance with information rights.

7.2 An audit from the ICO will be requested by the NCA annually, to be agreed at a mutually suitable time and subject to both parties' available resources.

7.3 The NCA will ensure that it can demonstrate to the ICO that the necessary processes and procedures are in place in relation to the necessity and proportionality of use, disclosure and retention of BPDs. In particular the NCA should ensure that it can establish to the satisfaction of the ICO that its policies and procedures in this area are (a) sound and provide adequate safeguards against misuse and (b) are strictly complied with, including through the operation of adequate protective monitoring arrangements.

7.4 The NCA must provide the ICO with all such documents and information as the latter may require for the purposes of enabling him/her to exercise the oversight described in paragraph 7.1 above.

## 8. Record Keeping and Error Reporting

8.1 The ABAM to whom a BPD Authorisation or BPD Disclosure Authorisation is addressed will be responsible for maintaining a local copy of all such authorisations together with all associated applications, reviews, renewals, modifications and cancellations.

8.2 The CDO will also maintain a centralised copy of all BPD Authorisations and BPD Disclosure Authorisations together with all associated applications, decisions of the Issuing Authority, renewals, modifications, cancellations and records of destruction.

8.3 The CDO will maintain a Master BPD Schedule detailing all BPDs retained by the NCA. The schedule will record the following detail and associated dates:

- Applications for BPD Authorisation;
- Applications for BPD Disclosure Authorisation;
- Applications for Class BPD Authorisation;
- Applications for Overarching Seized Device Data BPD Authorisation;
- Which applications are authorised;
- Which applications are rejected;
- Renewals;
- Modifications;
- Use of the urgent process;
- Cancellations;
- Records of destruction.

8.4 An error may occur where a BPD dataset is obtained, retained or examined in breach of the Data Protection Act 2018 and/or Article 8 ECHR resulting in an unjustifiable interference with privacy.

8.5 Any failure by NCA officers to apply the correct processes set out in this Operating Procedure will increase the likelihood of an error occurring. Errors can have significant consequences on affected individuals' rights. Wherever possible, technical systems should incorporate functionality to minimise errors.

8.6 This Operating Procedure cannot provide an exhaustive list of possible errors that would fall within paragraph 8.4, however examples could include:

- Retaining or examining a dataset beyond the initial examination period without BPD authorisation;
- use of an initial examination period where it is not permitted because of circumstances outlined in paragraph 10.3;

- use of multiple initial examination periods for the same BPD by different parts of the NCA;
- operational exploitation or intelligence development of a BPD during the initial examination period;
- disclosure of a BPD without a BPD Disclosure authorisation;
- washing other data against an authorised BPD if this is not permitted by the terms of the existing BPD authorisation; or
- failing to seek a Specific BPD Authorisation for a dataset which consists of or includes protected data, health records, or is novel or contentious.

8.7 An error may be classified as minor, moderate or serious:

(a) A minor error is one that carries a low risk of prejudice to the rights and freedoms of individuals under DPA 2018/Article 8 ECHR.

(b) A moderate error is one where there is a medium risk to the rights and freedoms of individuals in the form of unjustifiable interference with privacy under DPA 2018/Article 8 ECHR.

(c) A serious error is one where there is a high risk of prejudice to the rights and freedoms of individuals in the form of unjustifiable and unauthorised interference with privacy under DPA 2018/Article 8 ECHR.

8.8 All errors will be clearly documented as minor, moderate or serious and reported to the DAP. The DAP panel will confirm the classification given, consider the impact of the error and address any pattern to the commission of errors.

The DAP will consider the sufficiency of the remedial measures outlined in all error reports and any lessons to be learned, this includes suitable routes for escalation. Serious errors will be escalated by the DAP panel to the Data Governance Board or Information Commissioner's Office, as appropriate.

8.9 From the point at which the NCA identifies an error may have occurred it will take steps to confirm the facts of an error as quickly as it is reasonably practicable to do so. Any potential errors must be flagged to the BPD Authorisations Team in CDO. A report will be prepared by Chief Data Office, for presentation to the DAP, to include:

- the cause of the error;
- amount of data retained, selected for examination or disclosed in error;
- any unintended or collateral intrusion;
- any analysis or action taken;
- whether the data has been retained or destroyed; and
- a summary of the steps taken to prevent recurrence.

8.10 Any errors or procedural deficiencies should be notified to the IAO and CDO. Any serious errors or deficiencies should also be brought to the attention of the Issuing Authority and Security and Standards Department. Any serious breaches of safeguards that have resulted in an unauthorised or unjustifiable interference with privacy will be subject to internal investigation and, where appropriate, reported to the ICO by the CDO.

8.11 The DAP must undertake a regular review of reported errors and lessons learned.

Part 2: The BPD life-cycle

9 Obtaining BPDs

9.1 The NCA may obtain BPDs through its information gateway or pursuant to other channels or statutory powers available to it.

9.2 A BPD Authorisation does not provide a capability to obtain data beyond that which is otherwise available to the NCA. However, the method by which a dataset was, or will be, obtained is a relevant factor for the Issuing Authority in deciding whether to issue a BPD Authorisation, and/or whether an Authorisation, is in fact, required.

9.3 Prior to obtaining a dataset, based on the information available to them at the time, NCA officers should consider whether a BPD Authorisation will be required for its retention and the selection of data for examination from that BPD. NCA officers should apply for a BPD Authorisation prior to the BPD being obtained if sufficient information is available to enable an informed assessment to be made that:

- the dataset is a BPD, and;
- the BPD is of a nature that the NCA would wish to:

  a) retain it;
  b) select data for examination from it, and/or;
  c) disclose it.

9.4 Where a dataset is obtained, and a BPD Authorisation has not already been sought, if it is believed that the dataset is, or may be, a BPD, the CDO must be notified and provided with:

(a) the date the dataset was obtained, and

(b) whether the dataset was retrieved/downloaded in the UK or outside of the UK.

An initial examination period may apply, this is discretionary and not available in every case (see section 10).

## 10. Initial Examination

10.1 The initial examination period is a time-limited preliminary stage (see 10.4) during which a potential BPD may be held without a BPD authorisation, in order to carry out an initial assessment of the quality of the dataset and the nature of the data content.

10.2 Where an NCA officer expects to obtain a dataset, whether solicited or unsolicited and believes it may require a BPD Authorisation, they should liaise with the BPD authorisations team to complete an Initial Assessment Form. An initial examination period is only applicable if a BPD Authorisation has not already been sought.

10.3 NCA officers may have a permitted period in which to undertake an initial examination of the dataset to assess:

- whether the dataset is a BPD, and/or;
- establish if the BPD is of a nature that the NCA would wish to:

a) retain it;
b) select data for examination from it, and/or;
c) disclose it.

Once the allocated dates of the initial examination period are confirmed with the NCA officer, data matches are allowed, however operational activity or intelligence development cannot take place.

10.4 The permitted period for undertaking the initial examination is:

- three months from the date of receipt of the dataset by the NCA if the dataset was retrieved/ downloaded in the UK, or;
- six months from the date of receipt of the dataset by the NCA if the dataset was retrieved/ downloaded outside of the UK.

These timescales represent a maximum permitted period and should not be viewed as a target deadline.

10.5 An NCA Officer will not be required to apply for a BPD authorisation, if it is established from the initial examination that the dataset is not a BPD.

10.6 If the dataset meets the criteria for a BPD, but the NCA does not wish to retain the entire dataset and/or disclose it, beyond the initial examination

period, the dataset must be deleted and destroyed as soon as possible (see section 14).

10.7 An initial examination can include processing a set of information which might otherwise meet the definition of a BPD, with a view to permanently deleting individuals within that dataset who are not, and are unlikely to become of intelligence interest, such that the dataset no longer meets the definition of a BPD. Once the deletion of individuals who are not subjects of interest is complete, the initial examination period ceases and the remaining data may be retained without a BPD authorisation.

This deletion of individuals who are not of interest must be done as soon as reasonably practicable and in any event within the permitted period. If it is already clear it will not be possible to permanently delete individuals who are not of interest within the initial examination period, a BPD authorisation must be sought for the dataset in advance of obtaining it. What is reasonably practicable will depend on the circumstances and the nature of the dataset. Where a dataset is in a foreign language, technically challenging, comes from overseas or requires separation, may justify a longer portion of the permitted period being used.

10.8 The deletion should be confirmed to the BPD Authorisation team and the ABAM or respective team managers. This should be carried out in line with NCA Information Management Policy and command level operating procedures.

10.9 Once the NCA officer confirms that the dataset meets the criteria for a BPD during the initial examination, and the NCA wishes to retain it, select data for examination from it, and/or disclose it, the initial examination must then cease and a BPD authorisation be sought (unless paragraph 10.6 applies). This will not apply to any existing Class BPD authorisations in place.

10.10 No further examination of the dataset is permitted once a decision has been made by the examining officer that the dataset is a BPD and is of a nature that NCA would wish to retain, examine, or disclose.

10.11 There are limited purposes for which an initial examination may be carried out. What may be done during an initial examination period is limited to the assessment set out in paragraph 10.3 and/or carrying out the deletion task set out in paragraph 10.7. During the permitted period, the selection of data for examination may only be carried out for the purpose of conducting the initial examination and not for any other purposes. Safeguards must be put in place by the ABAM to limit access to the data strictly to those carrying out the initial examination.

10.12 The initial examination period is not available in all cases and should not be used where:

- an NCA officer knows prior to receipt that the dataset is a BPD and NCA would wish to retain it, select data from it for examination, or disclose it; or
- the NCA has previously received a dataset of a similar nature.

10.13 An NCA officer must complete this initial examination as soon as reasonably practicable and, in any event, within the permitted period. The initial examination period should be commenced and completed without unreasonable delay. Unreasonable delays in conducting an initial examination (therefore retention of a dataset without BPD authorisation) may result in an error under this OP and potential breach of Article 8 ECHR and/or the Data Protection Act 2018.

10.14 A BPD authorisation must be sought if it is not possible to permanently delete individuals who are not of interest during the course of the initial examination period, activity concerning the entire dataset must cease. This applies as soon as NCA officers decide it will not be possible to complete the deletion within the timescale of an initial examination period. In the BPD authorisation application, the applicant must candidly explain what was done during the initial examination period and why it is not possible to complete the deletion exercise within the permitted period.

10.15 If a BPD Authorisation is not sought within the permitted period, the BPD should be destroyed (see section 14).

## 11. Selection of Data for Examination

*Selection for examination*

11.1 No data retained under a BPD Authorisation can be selected for examination[15], other than for the purposes of the initial examination, unless this is authorised under the BPD Authorisation.

11.2 Where a third party allows an NCA officer access to a BPD (a) that the third party retains, and (b) for which the third party is the data controller, no authorisation is required by the NCA to select data for examination.

[15] For the purposes of this Operating Procedure, the selection of data includes the:
(1) organisation, adaptation or alteration of data from the BPD;
(2) retrieval, consultation or use of data from the BPD; and
(3) alignment or combination of data from the BPD with other information or datasets.

11.3 Where a BPD retained by the NCA will be made available to a third party to select data for examination this may amount to a disclosure and must be reflected in the NCA's BPD Authorisation and where appropriate a BPD Disclosure Application (IM01 F30). The application must clearly state which third parties will have access and detail how the selection for examination safeguards will be applied by the third party.

11.4 A BPD Authorisation can only be issued to select data for examination where it is necessary and proportionate to examine that data for one or more 'operational purposes'. These operational purposes must be specified in the BPD Authorisation.

11.5 A list of operational purposes is contained at Annex C. This list will be reviewed regularly by the DAP and any amendments require approval of the DGC. Operational purposes must:

- be in furtherance of the NCA's functions;
- contain greater detail than the necessity grounds for authorisation;
- give the Issuing Authority a clear understanding of what data will be selected for examination, in order to allow for a proper assessment as to necessity and proportionality.

11.6 A BPD Authorisation can, within a given operational purpose, provide a more detailed description of the purpose for which data will be selected where this allows for a better assessment as to necessity and proportionality. For example, where the data selected for examination is for the purpose of a specific NCA Campaign.

11.7 If an NCA officer needs to select data for examination for purposes other than one of the operational purposes specified in the BPD Authorisation, a modification to that authorisation must be sought.

*Examination*

11.8 A BPD may only be examined[16] if:

a) the examination in question falls within the specified 'operational purposes' approved under the relevant BPD Authorisation, and;

b) the officer in question is satisfied that the particular examination is both necessary and proportionate. The officer examining a BPD is required to record the necessity and proportionality justifications for each examination in writing.

[16] For the purposes of this Operating Procedure the examination of data means reading, looking at or listening to data by the persons to whom it becomes available as a result of the data being selected from a BPD under a BPD Authorisation.

11.9 Whether any particular examination of a BPD is necessary and/or proportionate is a matter of judgement, taking all relevant circumstances into account. The officer must consider whether the examination that is proposed is 'really needed', and must balance the seriousness of the intrusion into privacy that will be caused by the examination against the investigative value that the examination is expected to produce. Consideration must always be given to whether there are other, less intrusive, means of achieving the same investigative end.

11.10 Where the examination of data selected pursuant to a BPD authorisation amounts to monitoring or observing persons, their movements, conversations or other activities and communications, consideration should be given to whether a surveillance authorisation is required.

11.11 The examination of data selected pursuant to a BPD authorisation is not limited to the specified operational purposes for which the data has been selected. Where it is necessary and proportionate to do so, that selected data can be examined for any other purpose in the exercise of any NCA function without the need for further authorisation.

11.12 Where the applicant anticipates that data selected for examination pursuant to a specified operational purpose will be examined for other purposes; this should be stated in the application as this may be relevant to the considerations of the Issuing Authority.

*BPD Authorisation*

11.13 The Issuing Authority may only issue a BPD Authorisation if the following conditions are met:

- The BPD Authorisation is necessary on one or more of the following grounds ("the necessity grounds"):

    a) for the purpose of preventing or detecting serious crime, or;
    b) for the purpose of preventing death or any injury or damage to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health.

- The conduct authorised is proportionate to what it seeks to achieve;
- If authorising the selection of data for examination, it is necessary to examine that data for each of the specified operational purposes, and;
- There are satisfactory safeguards in place, including arrangements for storing the BPD and for protecting it from unauthorised disclosure in accordance with the requirements of this Operating Procedure.

11.14 In deciding whether to issue, renew, modify or cancel a BPD Authorisation, the Issuing Authority must have regard to:

- whether what is sought to be achieved could reasonably be achieved by other less intrusive means;
- whether the level of protection applied in relation to the BPD is higher because of the particular sensitivity of the data, and;
- any other aspects of the public interest in the protection of privacy.

*Necessity*

11.15 What is necessary in a particular case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the 'necessity' requirement, the NCA must consider why retention of the BPD is 'really needed' for the specified necessity grounds and, for selection for examination, the specified operational purposes (see paras 11.7 – 11.9).

*Proportionality*

11.16 Any assessment of proportionality involves balancing the seriousness of the intrusion into privacy against the need for the activity in investigative, operational or capability terms.

11.17 The retention and/or selection for examination of the BPD must also be proportionate to what is sought to be achieved by the conduct authorised. In order to meet the 'proportionality' requirement, the Issuing Authority must balance:

- the level of interference with the individual's right to privacy (and any other rights that might be enjoyed depending on the circumstances), both in relation to subjects of interest who are included in the relevant data and in relation to other individuals who are included in the dataset and who may be of no interest to the NCA in the exercise of its functions, against;

- the expected value to be derived from the dataset in the furtherance of the necessity grounds and, for selection for examination, the specified operational purposes.

11.18 The Issuing Authority must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the dataset and the importance of the operational purposes to be achieved.

11. 19 The Issuing Authority must also consider whether there is a reasonable alternative that will still meet the proposed objective and which involves less intrusion. An authorisation will not be proportionate if it is excessive in the overall circumstances of the case. The conduct authorised should bring an expected benefit to the exercise of the NCA's functions and should not be

disproportionate or arbitrary. The fact that there is a potential threat to life (for example) may not necessarily render intrusive conduct proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

*Intrusiveness of Data*

11.20 When considering whether it is proportionate to grant a BPD Authorisation, the Issuing Authority will assess the degree or extent of the intrusiveness which retaining or examining the BPD would involve, that is to say the degree or extent of interference with individuals' right to privacy under Article 8 of the European Convention on Human Rights[17].

11.21 The intrusiveness of each dataset is assessed on a case-by-case basis, and in the round, having regard (amongst other things) to the following factors or indicators:

- Is there an expectation of privacy? Did the individual provide their personal data in confidence to another organisation, not expecting that anyone except that organisation would have access to their data?
- Does the data consist of more than basic personal details (e.g. more than name, date of birth, address, telephone number and e-mail address)?
- Is there information on a person's activities or movements or travel?
- Does the data include:
    i. protected data?
    ii. substantial proportion of data amounts to sensitive processing?
    iii. health records?
    iv. confidential information relating to members of sensitive professions or journalistic sources?
    v. data that attracts legal professional privilege?
- To what degree does the data, by virtue of its quality, nature or size, mean that, when it is examined, there will be a significant degree of intrusion into the privacy of individuals not of interest to the NCA in the exercise of its functions?

11.22 These indicators are not intended to be prescriptive; the presence of one or more will not necessarily result in the dataset as a whole being considered to be relatively more intrusive.

[17] Article 8 provides that everyone has the right to respect for his private and family life, his home and correspondence. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

When considering seeking authorisation of a new BPD, NCA officers must:

* consider the reasons why it is necessary to retain/examine the data;
* consider the proportionality of retaining/examining the dataset in particular, officers must consider whether there is a less intrusive way of obtaining the same intelligence benefit;
* consider the level of intrusion, direct or collateral in the NCA retaining/examining the proposed dataset;
* ensure the relevant form process is adhered to and has been authorised.

*Safeguards*

11.23 The NCA attaches the highest priority to maintaining information security and protective security standards, including:

- Physical security to protect any premises where BPDs may be accessed;
- IT security to minimise the risk of unauthorised access to IT systems and BPDs, and;
- A security-clearance regime for personnel to provide assurance that those who have access to BPDs are reliable and trustworthy.

11.24 In relation to information held in BPDs, the application must demonstrate that the following additional safeguards are in force and the Issuing Authority must consider that the specified safeguards are sufficient before any BPD Authorisation can be issued:

- Access to and examination of the information contained within BPDs is strictly limited to those with an appropriate business requirement to use the data;
- NCA officers may only select for examination information within a BPD if examination of the BPD is necessary on one or more of the necessity grounds and for one or more of the operational purposes specified in the BPD Authorisation;
- If NCA officers access information within a BPD with a view to subsequent disclosure of that information, they may only select and examine the relevant information if such disclosure is necessary for the performance of the NCA's functions or is otherwise permitted by its information gateways;

- Before accessing or disclosing information, NCA officers will consider whether to do so would be proportionate, including whether other, less intrusive, methods can be used to achieve the desired outcome;

- Users of BPDs will receive training regarding their professional and legal responsibilities, including the application of this Operating Procedure. Refresher training and/or updated guidance will be provided when systems or policies are updated;

- There is a system in place for effectively monitoring the examination of BPDs by NCA officers, in order to detect misuse or identify activity that may give rise to security concerns;

- Appropriate disciplinary action is taken in the event of inappropriate behaviour being identified, and;

- Users are warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which could include dismissal and prosecution[18].

11.25 In relation to the officers selecting data for examination, the NCA will ensure that the following measures are taken to reduce the level of interference with privacy arising from the retention and examination of BPDs:

- Minimising the number of results which are presented for examination, by training and requiring officers to frame queries in a proportionate way, and;

- If necessary, confining access to specific datasets (or subsets thereof) to a limited number of officers.

11.26 The NCA will maintain an audit capability for the systems used to retain BPDs or select data for examination for those BPDs. Use of BPDs by NCA officers will be monitored in order to detect misuse or identify activity that may give rise to security concerns. This includes carrying out periodic audits to ensure that the requirements set out in this Operating Procedure are being met. These audits must include checks to ensure that the documentation justifying selection for examination has been correctly compiled with and, specifically, that selection for examination of data was for an operational purpose specified in the BPD Authorisation. Any such identified activity will initiate the NCA's error reporting process (see para 8.4 – 8.6).

[18] For example, for an offence contrary to s170 DPA 2018 (unlawful obtaining etc. of personal data).

*Additional safeguards for certain categories of data*

11.27 Where the BPD contains, or is reasonably believed to contain, certain categories of data, additional safeguards apply. These categories of data and the relevant safeguards, including protected data and confidential information relating to sensitive professions. These are set out in detail at Annex D.

12. Review and renewal of retention and selection of data for examination

12.1 When an ABAM is conducting a review (see para 6.18) or the Issuing Authority is considering an application for renewal (see para 6.19), as a minimum, consideration must be given to the following factors:

- The operational and legal justification for continued retention and selection for examination, including its necessity and proportionality (by reference to the requirements at paras 11.15 - 11.19);
- Whether such information could be obtained elsewhere through less intrusive means;
- An assessment of the value derived to date from the dataset and details of data selected for examination. If no selection for examination has taken place, an explanation as to why this is the case and when selection for examination is likely to occur. In light of these considerations, an assessment should be made of the on-going value of retaining the dataset;
- The extent to which the dataset originally acquired needs to be replaced by a more up-to-date dataset;
- The level of intrusion into privacy;
- The extent of political, reputational or other risk, and;
- Whether any caveats or restrictions should be applied to continued retention.

12.2 Where the continued retention of a BPD no longer meets the tests of necessity and proportionality, the authorisation for retention must be cancelled and the BPD destroyed (see para 14.0).

13. Disclosure

13.1 A BPD (or a subset itself amounting to a BPD) cannot be disclosed to persons outside of the NCA without a BPD Disclosure Authorisation (IM01 F30).

13.2 An NCA officer can apply for a BPD Authorisation for the limited purpose of disclosing a BPD to a third party. A BPD Authorisation of this type will not permit the NCA to retain or examine a copy of the BPD. This may be appropriate, for example, when it is not necessary or proportionate for the NCA to retain a copy of the BPD but there is a clear benefit to the discharge of the NCA's functions in disclosing the BPD to a third party.

*BPD Disclosure Authorisation*

13.3 The Issuing Authority may only issue a BPD Disclosure Authorisation if:

- the objective of the disclosure falls within a permitted purpose[19] or is made in accordance with intelligence service disclosure arrangements;
- it is necessary to disclose the information in question in order to achieve that objective;
- the disclosure is proportionate to the objective;
- only as much of the information will be disclosed as is necessary to achieve that objective, and;
- reasonable steps have been taken to ensure that the intended recipient organisation has, and will maintain, satisfactory arrangements (a) regarding the use of the BPD, (b) for safeguarding the confidentiality of the data and (c) for ensuring that it is securely handled, including storage of the BPD and protecting it from unauthorised disclosure.

*Necessity*

13.4 In order to meet the 'necessity' requirement in relation to disclosure, the Issuing Authority must be satisfied that disclosure of the BPD is 'really needed' to meet the objective of that disclosure.

*Proportionality*

13.5 The disclosure of the BPD must also be proportionate to the objective in question. In order to meet the 'proportionality' requirement, the Issuing Authority must be satisfied that the level of interference with the individuals'

[19] 'Permitted purpose' shall have the same meaning as provided in section 16 of the CCA

right to privacy is justified by the benefit which is expected as a result of disclosing the data and the importance of the objective to be achieved. The Issuing Authority must consider whether there is a reasonable alternative that will still meet the proposed objective – i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole BPD.

*Intrusiveness of data*

13.6 When considering whether it is proportionate to grant a BPD Disclosure Authorisation, the Issuing Authority will assess how 'intrusive' the dataset is, that is to say the degree or extent of interference with individuals' right to privacy under Article 8 ECHR. In doing so, the Issuing Authority will have regard to the indicators at para 11.21.

*Safeguards*

13.7 Before disclosing any BPDs, the NCA must take reasonable steps to ensure that the intended recipient organisation has, and will maintain, satisfactory arrangements regarding the:

a) use of the BPD;
b) safeguarding of the confidentiality of the data, and;
c) ensuring that it is securely handled, including storage of the BPD and protecting it from unauthorised disclosure.

13.8 What is reasonable will depend on the circumstances of the case, but will include consideration of the nature of the disclosure and what is known about the recipient.

*Additional safeguards*

13.9 Where the BPD contains, or is reasonably believed to contain, certain categories of data, additional safeguards apply. These categories of data and the relevant safeguards are set out at Annex D.

## 14. Destruction

14.1 All copies of BPDs held by the NCA should be destroyed when:

- The permitted period for initial examination has expired;
- A BPD Authorisation for retention is refused, or;
- A BPD Authorisation for retention is cancelled (or not renewed).

14.2 For the purposes of this Operating Procedure, destruction of data means the deletion of the data in such a way as to make access to the data by an NCA officer or agent of the NCA impossible.

14.3 Where data cannot be immediately destroyed, the NCA must ensure the data is scheduled for deletion and securely destroyed as soon as practicable. In this context, this means taking such steps as might be necessary to make access to the data unavailable to NCA officers pending destruction.

14.4 On completion, the IAO for the BPD must provide a record of destruction to the relevant issuing authority (via the CDO).

14.5 This requirement does not require the destruction of data selected for examination (where that dataset does not itself amount to a BPD) or intelligence derived from the BPD.

14.6 A BPD can be retained or examined without a BPD Authorisation (or following cancellation of an authorisation) for the sole purpose of enabling the BPD to be destroyed.

Related Documents
IM01 Managing NCA Information
IM01 OP04 Review, Retention and Disposal of NCA Information
IM01 OP06 Disclosing NCA Information

IM01 F02 BPD Initial Application
IM01 F03 Application for BPD Renewal
IM01 F04 Application for BPD Cancellation
IM01 F30 Application for BPD Disclosure
IM01 F37 BPD Initial Assessment Form
IM01 BPD Authorisation Certificate
IM01 F51 BPD Record of Deletion Form
IM01 F58 BPD Error Reporting Form
IM01 F56 BPD Application Update
IM01 F54 Application for Class Bulk Personal Dataset
IM01 F62 Overarching Application for Secondary Use of Seized Device Data
IM01 F60 Specific Request for Secondary Use of Seized Device Data
IM01 F61 Overarching Application for Secondary Use of Seized Device Data Renewal

METADATA

Operating Procedure Ownership

| | |
|---|---|
| Director Owner | Chief Information Officer |
| Deputy Director Owner | Chief Data Officer |
| Responsible Team | BPD Team, Chief Data Office |
| Version Control | V1.0 30/11/2017 |
| Version Control | V2.0 18/04/2019 |
| Version Control | V3.0 03/07/2019 |
| Version Control | V4.0 19/08/2019 |
| Version Control | V5.0 30/10/2019 |
| Version Control | V6.0 29/09/2022 |
| Version Control | V7.0 27/07/2023 |
| Version Control | V8.0 04/03/2024 |
| Version Control | V9.0 03/03/2025 |

National Crime Agency

Annex A - DEFINITIONS:

'acquisition' means any lawful method used to obtain or access the dataset.

'civil proceedings' means any proceedings in or before any court or tribunal that are not criminal proceedings.

'confidential information relating to sensitive professions' is explained in Annex D para 2.3 -2.5.

'confidential journalistic material' means:

a) in the case of material contained in a communication, journalistic material which the sender of the communication:

   i. holds in confidence, or;
   ii. intends the recipient, or intended recipient, of the communication to hold in confidence.

b) in any other case, journalistic material which a person holds in confidence.

A person holds material in confidence if:

a) the person holds it subject to an express or implied undertaking to hold it in confidence, or;
b) the person holds it subject to a restriction on disclosure or an obligation of secrecy contained in an enactment.

See also 'Journalistic Material'

'crime' means conduct which:

a) constitutes one or more criminal offences, or;
b) is, or corresponds to, any conduct which, if it all took place in any one part of the United Kingdom, would constitute one or more criminal offences.

'data' includes data which is not electronic data and any information (whether or not electronic).

'dataset' means any set of information in any format.

'destroy', in relation to electronic data, means delete the data in such a way as to make access to the data impossible (and related expressions are to be read accordingly).

'detecting serious crime' includes:

a) establishing by whom, for what purpose, by what means and generally in what circumstances any serious crime was committed, and;
b) the apprehension of the person by whom any serious crime was committed.

'examination' means viewing, processing or analysing the dataset.

'health records' means a record, or a copy of a record, which:

a) consists of information relating to the physical or mental health or condition of an individual;
b) was made by or on behalf of a health professional in connection with the care of that individual, and;
c) was obtained by the NCA from a health professional or a health service body or from a person acting on behalf of a health professional or a health service body in relation to the record or the copy.

'identifying data' means:

a) data which may be used to identify, or assist in identifying, any person, apparatus, system or service,
b) data which may be used to identify, or assist in identifying, any event, or;
c) data which may be used to identify, or assist in identifying, the location of any person, event or thing.

'items subject to legal privilege' (always consult Legal immediately if legal privilege material may be involved):

a) In relation to England and Wales, has the same meaning as in the Police and Criminal Evidence Act 1984 (section 10 of that Act),

b) In relation to Scotland, means:

   i. communications between a professional legal adviser and the adviser's client, or;
   ii. communications made in connection with, or in contemplation of, legal proceedings and for the purposes of those proceedings, which would, by virtue of any rule of law relating to the confidentiality of communications, be protected in legal proceedings from disclosure.

c) In relation to Northern Ireland, has the same meaning as in the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989/1341 (N.I. 12)) (see Article 12 of that Order).

'journalistic material' means material created or acquired for the purposes of journalism.

*Note: For the purposes of clarity where:*

*a) a person ('R') receives material from another person ('S'), and;*
*b) S intends R to use the material for the purposes of journalism,*
*R is to be taken to have acquired it for those purposes. Accordingly, a communication sent by S to R containing such material is to be regarded as a communication containing journalistic material.*

For the purposes of determining whether a communication contains material acquired for the purposes of journalism, it does not matter whether the material has been acquired for those purposes by the sender or recipient of the communication or by some other person:

a) material is not to be regarded as created or acquired for the purposes of journalism if it is created or acquired with the intention of furthering a criminal purpose, and;
b) material which a person intends to be used to further such a purpose is not to be regarded as intended to be used for the purposes of journalism.

(see also *'confidential'* journalistic material)

'legal proceedings' means:

c) civil or criminal proceedings in or before a court or tribunal, or;

d) proceedings before an officer in respect of a service offence within the meaning of the Armed Forces Act 2006.

'modify' includes amend, repeal or revoke (and related expressions are to be read accordingly).

'NCA Functions' means statutory functions of the NCA, the DG NCA and other NCA officers[20]. – see also Annex C.

'NCA Officers' means:

a) the Director General;
b) the other National Crime Agency officers appointed under paragraph 9 of Schedule 1;
c) persons who have been seconded to the NCA to serve as National Crime Agency officers under paragraph 13 of Schedule 1 (unless the context otherwise requires), and;
d) NCA specials.

'of interest' means of legitimate law enforcement interest to the NCA in relation to NCA functions and operational purposes and NCA administrative functions (HR records etc.).

[20] See section 16 CCA.

'personal data' has the same meaning as in the Data Protection Act 2018 except that it also includes data relating to a deceased individual where the data would be personal data within the meaning of that Act if it related to a living individual.

'permitted purpose' in respect of the NCA only means:

a) the prevention or detection of crime, whether in the United Kingdom or elsewhere;

b) the investigation or prosecution of offences, whether in the United Kingdom or elsewhere;

c) the prevention, detection or investigation of conduct for which penalties other than criminal penalties are provided under the law of any part of the United Kingdom or the law of any country or territory outside the United Kingdom;

d) the exercise of any NCA functions (so far as not falling within any of paragraphs (a) to (c);

e) purposes relating to civil proceedings (whether or not in the United Kingdom) which relate to a matter in respect of which the NCA has functions;

f) compliance with an order of a court or tribunal (whether or not in the United Kingdom);

g) the exercise of any function relating to the provision or operation of the system of accreditation of financial investigators under section 3 of the Proceeds of Crime Act 2002;

h) the exercise of any function of the prosecutor under Parts 2, 3 and 4 of the Proceeds of Crime Act 2002;

i) the exercise of any function of the:

- Director of Public Prosecutions;
- Director of the Serious Fraud Office;
- Director of Public Prosecutions for Northern Ireland, or;
- Scottish Ministers, under, or in relation, to Part 5 or 8 of the Proceeds of Crime Act 2002;

j) the exercise of any function of:

- an officer of Revenue and Customs;
- a general custom official;
- a customs revenue official;
- an immigration officer;

- an accredited financial investigator, or;
- a constable, under Chapter 3 of Part 5 of the Proceeds of Crime Act 2002;

k) investigations or proceedings outside the United Kingdom which have led, or may lead, to the making of an external order (within the meaning of section 447 of the Proceeds of Crime Act 2002);

l) the exercise of any function of any intelligence service (within the meaning of the Regulation of Investigatory Powers Act 2000);

m) the exercise of any function under:

- Part 2 of the Football Spectators Act 1989, or;
- sections 104 to 106 of the Policing and Crime Act 2009;

n) the exercise of any function relating to public health;

o) the exercise of any function of the Financial Services Authority;

p) the exercise of any function designated by the Secretary of State by order; but a function may be designated under paragraph (p) only if the function appears to the Secretary of State to be a function of a public nature.

'retention' means the storage of the dataset on an NCA electronic system.

'sensitive professions' includes lawyers, doctors/health professionals, journalists, Members of a relevant legislature, and Ministers of religion (Further detail can be found in Annex D paragraph 2).

'serious crime' means crime where:

a) the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or
b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

'source of journalistic information' means an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used.

'specific operational purpose' in relation to a class BPD authorisation or a specific BPD authorisation means the operational purposes specified in 'Annex C – Operational Purposes' of this Operating Procedure.

'systems data' means any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following:

a) a postal service;
b) a telecommunication system (including any apparatus forming part of the system);
c) any telecommunications service provided by means of a telecommunication system;
d) a relevant system (including any apparatus forming part of the system);
e) any service provided by means of a relevant system.

*Note: a system is a 'relevant system' if any communications or other information are held on or by means of the system.*

'UKIC' means the UK Intelligence Community.

'working day' means a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a bank holiday specified in Schedule 1 of the Banking and Financial Dealings Act 1971.

Annex B - Categorising data in BPD

2. Background

This Annex sets out a scheme for categorising data contained in a BPD.

1.1 The categorisation of data in a BPD determines:

a) whether a Specific BPD Authorisation or Class BPD Authorisation is required to retain and select data for examination, and;
b) whether additional safeguards are required.

3. Protected Data

2.1 Protected data means any data contained in a BPD other than data which is one or more of the following:

a) Systems data;
b) Identifying data that can be logically separated from the BPD and not reveal the meaning of the remaining data or BPD, or;
c) Data which is not private information.

2.1 For the avoidance of doubt, these categories of data are not mutually exclusive and provided the data falls within one of these categories it will fall outside the meaning of protected data.

Systems data

2.2 'Systems data' has the same meaning as in section 263 of the IPA (see also Annex A).

2.3 In summary, systems data is any data that enables or facilitates the functioning of any system or service. It includes all data that a system requires to function and provide its services.

2.4 For example, if a passport number in a flight booking system has to be valid for the passenger to be able to fly then that passport number, in that specific BPD will be systems data. The passport number will also be identifying data (see below).

Identifying data

2.5 'Identifying data' has the same meaning as in section 263 of the IPA (see also Annex A).

2.6 In summary, 'Identifying data' is data that may help to identify persons, systems services, locations or events. Accordingly, identifying data in a BPD does not need, of itself, to identify a person, systems service, location or event *provided* it is of assistance in doing so. For example, a person's name, address, occupation and country of birth in a BPD are each identifying data – although any one of them, on its own, might not identify a person, they are each data which may assist in doing so.

2.7 Identifying data does *not* constitute protected data where:

a) it is contained in the BPD;
b) it is capable of being logically separated from the BPD, and;
c) if it were so separated, it would not reveal anything of what might reasonably be considered to be the meaning (if any) of any of the data which would remain in the BPD or of the BPD itself, disregarding any meaning arising from the existence of that data or (as the case may be) the existence of the BPD or from any data relating to that fact.

2.8 If an individual data item meets these conditions then it should be categorised as identifying data in its own right. The categorisation of the data from which it was derived remains unaffected (and could constitute protected data). Accordingly, protected data may contain data items that individually constitute identifying data.

Private information

2.9 Private information includes information relating to a person's private or family life.

2.10 For example, in the BPD context, information which is non-private *may* include:

- publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, mapping imagery, commercial subscription databases, academic articles, conference proceedings, business reports, etc;

- data which is publicly accessible online where there is no expectation of privacy over that information, for example Companies House (by contrast information posted on personal social network sites accessible by personal contacts, may include some information where an expectation of privacy might apply);

- commercially available data where a fee may be charged;

- data which is available on request or made available at a meeting to a member of the public;

- the attributes of inanimate objects, such as the class to which a cargo ship belongs.

3 Health Records

3.1 A health record has the same meaning as in section 206(6) of the IPA, namely a record, or a copy of a record, which:

a) consists of information relating to the physical or mental health or condition of an individual;
b) was made by or on behalf of a health professional in connection with the care of that individual, and;
c) was obtained by the NCA from a health professional or a health service body or from a person acting on behalf of a health professional or a health service body in relation to the record or the copy.

4 Sensitive processing means the processing of data which would be sensitive processing under section 35(8) of the Data Protection Act 2018. This means the processing of:

a) personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs or trade union membership;
b) genetic data, for the purposes of uniquely identifying an individual;
c) biometric data, for the purpose of uniquely identifying an individual;
d) data concerning health;
e) data concerning an individual's sex life or sexual orientation.

5 Limitations on use of Class BPD Authorisations

5.1 As set out in paragraph 6.6 of the Operating Procedure, a Class BPD Authorisation cannot be issued if:

a) the BPD consists of, or includes, protected data;
b) the BPD consists of, or includes, health records;
c) a substantial proportion of the BPD consists of personal data the processing of which would be sensitive processing within the meaning of s35(8) of the DPA 2018, or;
d) the nature of the BPD, or the circumstances in which it was created, is or are such that its retention or examination raises novel or contentious issues which ought to be considered by a Specific BPD Authorisation.

In assessing whether a Class BPD Authorisation would be available, NCA officers should adopt the practical approach set out in the flow-chart attached to this Annex.

Annex C – Statutory Function and Operational Purpose

1. Background

1.1 A BPD Authorisation can only be issued to select data for examination where it is *necessary* to examine the data for one or more statutory functions and operational purposes.

1.2 Each authorisation must specify:

a) Which statutory function the NCA is exercising (e.g. criminal intelligence function and or crime reduction function), and;
b) Which broad level operational purpose (see 2 below) the exercise of that function relates to.

1.3 The broad level operational purposes will be reviewed regularly by the DAP and any amendments require approval of the DGC.

2 Broad Level Operational Purposes

2.1 The following broad level operational purposes have been approved by the DGB.

a) Child sexual exploitation and abuse
b) Organised immigration crime
c) Cyber crime
d) Firearms
e) Money laundering
f) Bribery, corruption and sanctions evasion
g) Drugs
h) Economic crime
i) Modern slavery and human trafficking
j) Organised acquisitive crime
k) Terrorism
l) Borders vulnerabilities
m) Criminal use of identity
n) Criminal use of internet technology
o) Foreign national offenders
p) Prisons and lifetime management

NCA Capability Enablers

q) Testing, maintaining or developing capabilities
r) Training officers

4. Example

3.1 The following are example formulations of operational purposes:

a) For the purpose of the exercise of the NCA's criminal intelligence function in relation to child sexual exploitation and abuse.

b) For the purpose of the exercise of the NCA's serious crime reduction function in relation to testing, maintaining or developing capabilities.

Annex D - Additional Safeguards

1. Protected Data

1.1 Where a BPD contains protected data, the application should contain as much information, and be as specific as is practically possible, in relation to the protected data in the BPD, including the nature and type of the data and any other factors that may be relevant when assessing the level of intrusiveness of the protected data.

1.2 This is with a view to ensuring that the Issuing Authority can:

a) assess whether the safeguards set out in the application (in accordance with paras 11.23 – 11.27 of the Operating Procedure) are adequate and sufficient to provide the necessary Article 8 protection for the selection for examination of the protected data in the dataset, and;
b) if the safeguards are not sufficient, attach conditions to the authorisation.

1.3 In particular, the application should include (so far as reasonably practicable) the following specific information:

a) a description of the structure and scope of the BPD and of the information contained within it, including the different data involved and the nature and categories of data captured in those data, and, in particular, whether those data contain confidential information relating to members of sensitive professions;
b) a description, to include as much detail as is practically possible, of the nature and extent of the data which, following the initial examination of the dataset, it is known or believed may contain protected data;
c) whether any of the protected data are the contents of e-mails, letters or other documents;
d) whether any of the protected data contain communications between a member of a relevant legislature and another person on constituency business;
e) any other factors that may be relevant to the Issuing Authority's assessment of the level of intrusiveness of the protected data in the BPD, including the extent of the expectation of privacy arising from the circumstances and context in which the protected data were included in the BPD;
f) an assessment of whether, having regard to the above factors, the authorisation should be issued unconditionally or only subject to such conditions as may be approved by the Issuing Authority.

1.4 The Issuing Authority must determine whether the safeguards set out in the application (in accordance with paras 11.23 – 11.27 of the Operating Procedure) are adequate and sufficient to provide the necessary Article 8 protections for the selection for examination of the protected data in the dataset.

1.5 The safeguards (in accordance with paras 11.23 – 11.27 of the Operating Procedure) are likely to be adequate and sufficient to provide the necessary Article 8 protections in cases where the BPD comprises a dataset containing protected data of a low level of intrusiveness. Where the Issuing Authority is satisfied that the selection for examination safeguards are sufficient, the Issuing Authority may issue the authorisation without conditions.

1.6 Where the Issuing Authority is not so satisfied, but would otherwise be minded to issue the authorisation, the Issuing Authority may attach conditions to the issue of the authorisation. Requirements may be suggested by the IAO.

1.7 Conditions may include – but are not limited to – one or more of the following requirements:

a) to obtain the prior written approval of the Issuing Authority;
b) to seek the prior approval of a senior officer;
c) to seek the prior approval of a senior officer independent of purpose for which the data is to be selected for examination; or
d) a prohibition on selecting for examination any protected fields in the BPD using particular criteria.

1.8 Where a condition is attached to an authorisation, prior approval could relate to selection for examination for: known individuals, individuals who are members of a group who share a common purpose or who are carrying on a particular activity, more than one individual where the authorisation is given in the context of a single operation or investigation.

1.9 Where the BPD contains protected data of differing levels of intrusiveness, or a range of data, and the Issuing Authority considers that only some of those data require the additional controls (or that a range of additional controls is required), the Issuing Authority may choose either:

a) to apply the additional controls only to those data which require the additional controls; or
b) to apply the additional controls to all the protected data contained in the dataset.

1.10 Where conditions are attached these much be satisfied before protected data retained in reliance on the authorisation may be selected for examination on the basis of criteria which relate to an individual known to be in the British Isles at the time of selection.

## 2. Sensitive Professions

2.1 Due regard must be given to whether the level of protection applied in relation to any selection of data for examination is higher because of the particular sensitivity of the information being selected.

2.2 This applies to confidential information relating to members of sensitive professions. A 'sensitive profession' for these purposes includes:

a) Lawyers – selection for examination of legally privileged protected data;
b) Doctors / health professional – selection for examination of material attracting patient confidentiality, for example medical records or details of consultations;
c) Journalists – selection for examination of confidential journalistic protected data and journalists' sources;
d) Members of a relevant legislature[21] – selection for examination of protected data relating to a member of a relevant legislature and constituency business;
e) Ministers of religion – selection for examination of protected data relating to conversations between an individual and a minister of religion acting in his or her official capacity, and where the individual being counselled is seeking, or the minister is imparting, forgiveness, absolution or the resolution of conscience with the authority of the divine being(s) of their faith.

Held in confidence

2.3 Information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence, or is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

2.4 Most BPDs do not include details which would identify someone as a member of a sensitive profession, and do not contain confidential information relating to the sensitive professions. Further, information relating to a member of a sensitive profession is not, in and of itself, considered confidential.

2.5 For example, it would not include the mere fact of membership of the profession, or basic biographical details of a member of the profession. Thus, the fact that a solicitor's telephone number appeared in a telephone directory, would not be considered confidential information.

Scenarios where additional safeguards are required:

2.6 There are two scenarios in which the examination of BPD could give rise to the need for additional protection for confidential information relating to members of sensitive professions:

a) Firstly, it is possible that a BPD which contains protected data could include confidential information relating to a member, or members, of a sensitive profession. In this context, confidential information would include the content of communications between the professional, acting in their professional

[21] References to a member of a relevant legislature include to a Member of either House of the UK Parliament, the Scottish Parliament, the National Assembly for Wales, the Northern Ireland Assembly and Member of the European Parliament elected for the United Kingdom

capacity, and another party, and any information which identified journalistic material. Thus, for example, it would include the content of communications between lawyer and client, doctor and patient, or MP and constituent. Such protected data could also include confidential information which identified a journalistic source. In those circumstances, by virtue of the fact that the BPD contains protected data, a Specific BPD Authorisation must be sought and the additional safeguards must be applied.

b) Secondly, there is a small possibility that selection for examination of data (whether or not it is protected data) from BPDs could reveal the sources of journalistic material. In circumstances where the selection for examination conducted by an authorised person is for the purpose of identifying a source of journalistic material, the additional safeguards must be applied.

Additional safeguards

2.7 Where an NCA officer selects data for examination with the intention of obtaining privileged or otherwise confidential information, the officer must give special consideration to necessity and proportionality, must take into account any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken when considering whether data should be selected for examination in such circumstances, including additional consideration of whether there might be unintended consequences of such examination and whether the public interest is best served by the data being selected for examination.

2.8 These protections do not apply where communications were made with the intention of furthering criminal purpose. If an NCA Officer considers this to be the case, legal advice must be sought.

2.9 Further safeguards also apply to certain data relating to specific sensitive professions. These are set out below.

3. Selection for examination of protected data relating to a member of a relevant legislature and constituency business

3.1 Where the intention is to acquire communications between a member of a relevant legislature and another person on constituency business, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered.

3.2 If the information is exchanged with a criminal purpose, then the information will not be considered confidential for the purposes of this Operating Procedure.

3.3 Where the NCA intends to select for examination protected data relating to a member of a relevant legislature, the Issuing Authority *must* impose a condition requiring its prior written approval.

3.4 In accordance with its accountability arrangements, where operational activity involving the NCA in the UK raises new legal risks or is novel or contentious, the NCA must consult Home Office officials as early as is practicable. In this context, consultation must take place prior to the Issuing Authority granting approval for the selection for examination of protected data relating to a member of a relevant legislature and constituency business.

3.5 Prior approval of the Issuing Authority must be obtained regardless of whether the member of the relevant legislature is inside or outside the British Islands at the time of the selection for examination.

3.6 Where constituency business information is retained or disseminated to a third party, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of the information, advice should be sought from Legal and before any further dissemination of the content takes place.

4. Selection for examination of protected data attracting legal privilege

4.1 For the purposes of this Operating Procedure, any communication – whether in the UK or overseas - between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the items do not form part of a professional consultation of the lawyer, or there is clear and compelling evidence that the 'furthering a criminal purpose' exemption applies. Where there is doubt as to whether the material is subject to legal privilege or over whether the material is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception, advice should be sought from NCA Legal.

4.2 Section 10 of the Police and Criminal Evidence Act 1984 describes those matters that are subject to legal privilege in England and Wales. In Scotland, the definition of matters subject to legal privilege contained in section 412 of the Proceeds of Crime Act 2002 should be applied. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.

4.3 Legal privilege does not apply to material held with the intention of furthering a criminal purpose (whether the legal adviser is acting unwittingly or culpably). But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so, such as advocates, barristers, solicitors or Chartered Legal Executives.

4.4 Selecting legally privileged protected material for examination is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) of the ECHR as well as engaging Article 8. The selection for examination of legally privileged protected data contained in BPDs (whether deliberately or otherwise) is therefore subject to additional safeguards.

Intending to select protected data attracting legal privilege

4.5 Where the purpose, or one of the purposes, is to select for examination protected data attracting legal privilege:

a) The prior written approval of the Issuing Authority must be Obtained, and;

b) The Issuing Authority must be informed of the reasons why it is considered necessary and proportionate for the selection for examination to take place.

4.6 The Issuing Authority may only give approval if:

a) There are specific arrangements for the handling, retention, use and destruction of items subject to legal privilege, and;

b) There are exceptional and compelling circumstances that make it necessary to authorise the search. Such circumstances will arise only in a very restricted range of cases, such as where necessary for the purpose of preventing death or serious injury or in the interests of national security, and the selection for examination is reasonably regarded as likely to yield intelligence necessary to counter the threat. The exceptional and compelling test can only be met when the public interest in obtaining the information outweighs the public interest in maintaining the confidentiality of legally privileged material, and where there are no other reasonable means of obtaining the information.

Likely to select protected data attracting legal privilege

4.7 Where the purpose is *not* to select for examination protected data attracting legal privilege but the selection is nevertheless *likely* to identify such data:

a) the prior written approval of the Issuing Authority must be obtained;

b) the Issuing Authority must be informed of the reasons why it is considered necessary and proportionate for the selection for examination to take place, and;

c) the Issuing Authority must be provided with an assessment of how likely it is that legally privileged protected data will be selected.

4.8 The Issuing Authority may only give approval if there are specific arrangements for the handling, retention, use and destruction of items subject to legal privilege.

Inadvertently and unexpectedly selecting protected data attracting legal privilege

4.9 In the event that legally privileged protected data are inadvertently and unexpectedly selected for examination:

a) the protected data so obtained must be handled strictly in accordance with the handling, retention and deletion requirements below;

b) appropriate steps must be taken to minimise access to those data;

c) the CDO must be informed, and;

d) no further protected data may be selected for examination by reference to the criteria used to select the data, unless approved by the Issuing Authority. (see para 11.14 of this procedure)

Handling, retention and deletion

4.10 NCA officers who examine protected data contained in BPDs must be alert to any data which may be subject to legal privilege.

4.11 Where it is discovered that legally privileged protected data have been obtained inadvertently, an early assessment must be made of whether it is necessary and proportionate to retain them. If not, the protected data should be securely destroyed as soon as possible.

4.12 Where protected data have been identified following examination as legally privileged:

a) NCA officers who have access to the BPDs in question must be alerted to the fact that the dataset contains legally privileged material;

b) consideration should be given to whether a review of the Specific BPD Authorisation is required, and;

c) the Issuing Authority must be informed of the fact that the dataset contains legally privileged material on any further application for renewal of the Specific BPD Authorisation and on cancellation.

4.13 In addition, where legally privileged protected data are recorded and retained separately from the BPD for purposes other than their destruction they should be clearly marked as subject to legal privilege. Such data should be retained only where it is necessary and proportionate to do so. They must be securely destroyed when their retention is no longer needed for the authorised statutory purposes. If

such data are retained, the Information Asset Owner must ensure adequate information management systems are in place to ensure that continued retention remains necessary and proportionate for those purposes.

Dissemination

4.14 Where any action on or further dissemination of protected data subject to legal privilege is proposed:

a) Legal must be consulted on the lawfulness (including the necessity and proportionality) of any such dissemination, and;

b) consideration should be given to whether a review of the Specific BPD Authorisation is required.

4.15 The Issuing Authority must be informed of the dissemination or any further application for renewal of the Specific BPD Authorisation and on cancellation.

4.16 The dissemination of legally privileged protected data to an outside body should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to remove the risk of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates, including other law enforcement authorities. In this regard civil proceedings include all legal proceedings before courts and tribunals that are not criminal in nature. Neither the Crown Prosecution Service lawyer nor any other prosecuting authority lawyer with

conduct of a prosecution should have sight of any legally privileged protected data, with any possible connection to the proceedings. In respect of civil proceedings, there can be no circumstances under which it is proper for any public authority to have sight of or seek to rely on legally privileged protected data in order to gain a litigation advantage over another party in legal proceedings.

4.17 In order to safeguard against any risk of prejudice or perceived abuse of process, public authorities must also take all reasonable steps to ensure that lawyers or policy officials with conduct of legal proceedings should not see legally privileged protected data relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, the public authority must seek independent advice from Counsel and, if there is assessed to be a risk that sight of such content could yield a litigation advantage, the direction of the Court must be sought.

5. Selection for examination of confidential journalistic protected data and journalists' sources

5.1 There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously. Accordingly, the NCA's approach to journalistic protected data and journalists' sources takes into account the need to protect the proper exercise of free speech, and reflects the role that journalists play in protecting the public interest.

5.2 An assessment of whether someone is a journalist should be made on all the facts and circumstances available at the time. Consideration should be given, in particular, to the frequency of the individual's relevant activities, the level of personal rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. The fact that a person uses social media tools to communicate does not, in itself, indicate that a person is a journalist or that he or she is likely to be holding confidential journalistic material.

5.3 Where material is created or acquired with the intention of furthering a criminal purpose, the material is not to be regarded as having been created or acquired for the purpose of journalism.

Confidential journalistic material

5.4 Confidential journalistic material means:

a) In the case of material contained in a communication, journalistic material which the sender of the communication – (i) holds in confidence, or (ii) intends the recipient, or intended recipient, of the communication to hold in confidence, and;

b) In any other case, journalistic material which a person holds in confidence.

5.5 Confidential journalistic material includes data acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking. Confidentiality can continue to attach to confidential journalistic material when it is sent to or held by a person who is neither the journalist nor the source (for example, a news editor who has been sent some notes by a journalist). Once material has been broadcast, no confidentiality can attach to the material so it is not confidential journalistic material.

Journalistic sources

5.6 A source of journalistic information is an individual who provides material intending the recipient to use it for the purpose of journalism or knowing that it is likely to be so used. Any reference to sources should be understood to include any person acting as an intermediary between a journalist and a source.

5.7 Searches for sources of journalistic information do not necessarily depend on the content of the BPD. Accordingly, in rare cases, searches for sources could be facilitated by the selection of data which is not protected data. Therefore, the safeguards that apply in relation to the identification of sources of journalistic material should be read as applying to any BPD which is authorised for selection for examination and not just those BPDs which contain protected data.

Intending to select protected data

5.8 Where the intention is to select for examination (i) confidential journalistic protected data or (ii) data intended to identify a source of journalistic information:

a) The prior written approval of the Issuing Authority must be obtained, and;

b) The Issuing Authority must be informed of the reasons why it is considered necessary and proportionate for the selection for examination to take place.

Likely to select protected data

5.9 Where the intention is *not* to select for examination (i) confidential journalistic protected data or (ii) data intended to identify a source of journalistic information, but the selection is nevertheless *likely* to identify such data:

a) The prior written approval of the Issuing Authority must be obtained;

b) The Issuing Authority must be informed of the reasons why it is considered necessary and proportionate for the selection for examination to take place;

c) The Issuing Authority must be provided with (a) an assessment of how likely it is that such data will be selected; and (b) any possible mitigation steps.

Handling, retention, deletion and dissemination

5.10 Confidential journalistic protected data which have been identified as such, and data which identifies a source of journalistic information, should be retained only where it is necessary and proportionate to do so. It must be securely destroyed when its retention is no longer needed for those purposes. If such data are retained other than for the purposes of their destruction, the IAO must ensure adequate information management systems are in place to ensure that continued retention remains necessary and proportionate.

5.11 Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential journalistic protected data, advice should be sought from Legal and before any further dissemination of the content takes place.

Annex E

Commonly Used Powers (for retention, exploitation and disclosure of information)

| Power | Provision[i] (Territorial Application) | Detail (Authoriser) |
|---|---|---|
| Police and Criminal Evidence Act 1984 | | |
| PACE Search Warrant | Section 8(2) Police and Criminal Evidence Act 1984 (E&W)[ii] | Seizure of evidence of an indictable offence discovered during the search of a premises authorised under a warrant (Justice of the Peace) |
| Search of premises post arrest | Section 18(2) Police and Criminal Evidence Act 1984 (E&W)[iii] | Seizure of evidence of an offence discovered during the search of premises post arrest (Designated NCA G3 in most cases; Designated NCA officer where subsection 5A conditions meet) |
| General seizure power | Section 19(2)-(4) Police and Criminal Evidence Act 1984 (E&W)[iv] | Seizure of evidence or items obtained in consequence of the commission of an offence where lawfully on the premises (Designated NCA officer) |
| Extension of seizure powers to computerised information | Section 20(1) Police and Criminal Evidence Act 1984 (E&W)[v] | Seizure of information stored in any electronic form and accessible from premises (Designated NCA officer) |
| Search of persons post arrest | Section 32(9) Police and Criminal Evidence Act 1984 (E&W)[vi] | Seizure of evidence of an offence discovered following the search of a person post arrest (Designated NCA officer) |
| PACE Production Order | Schedule 1 paragraph 4, in conjunction with section 9, Police and Criminal Evidence Act 1984 (E&W)[vii] | Production order for excluded material or special procedure material (Judge) |
| PACE Excluded or Special Material Search Warrant | Schedule 1 paragraph 13, in conjunction with section 9, Police and Criminal Evidence Act 1984 (E&W)[viii] | Seizure of evidence discovered during the search of a premises authorised under a warrant for excluded or special procedure material (Judge) |
| Proceeds of Crime – Investigatory Orders | | |
| POCA Production Order | Section 345(4) (E&W, NI) / Section 380(5) (Scotland) Proceeds of Crime Act 2002 | Production order for material for a POCA investigation (Judge) |
| POCA Search and Seizure Warrant | Section 352(4) (E&W, NI) / Section 387(4) (Scotland) Proceeds of Crime Act 2002 | Seizure of material discovered during the search of a premises authorised under a warrant for a POCA investigation (Judge) |
| Extension of seizure powers to computerised information | Section 356(5) (E&W, NI) / Section 397(6) (Scotland) Proceeds of Crime Act 2002 | Seizure of information stored in any electronic form and accessible from premises relevant to a POCA investigation (Judge) |
| POCA Disclosure Order | Section 357(4) (E&W, NI) / Section 391(4) (Scotland) Proceeds of Crime Act 2002 | Disclosure order requiring disclosure of information relevant to a POCA investigation (Judge) |

| | | |
|---|---|---|
| POCA Customer Information Order | Section 363(5) (E&W, NI) Section 397(6) (Scotland) Proceeds of Crime Act 2002 | Customer information order requiring financial institution to disclose customer information relevant to a POCA investigation (Judge) |
| POCA Unexplained Wealth Order | Section 362A(3) (E&W, NI) / Section 396A(3) (Scotland) Proceeds of Crime Act 2002 | Unexplained wealth order requiring respondent to explain their interest in property (Judge) |
| POCA Account Monitoring Order | Section 370 (E, W &NI)/ Section 404 (Scotland) Proceeds of Crime Act 2002 | Monitoring bank account activity pursuant to a POCA investigation (Judge) |
| Other overt police powers | | |
| Seize and sift | Section 50 and 51 Criminal Justice and Police Act 2001 (UK) | Seizure of material from premises (s.50) or person (s.51) where there is a lawful power of seizure but it is not reasonably practicable to determine whether what he has found is |
| SOCPA Disclosure Notices | Section 62(3) Serious Organised Crime and Police Act 2005 (UK) | Information provided pursuant to a SOCPA disclosure notice (Crown Prosecutor) |
| IIOC Warrant | Section 4(2) Protection of Children Act 1978 (E&W)[22] | Seizure of indecent images of children following a warrant (Justice of the Peace) |
| Extraction of Information from electronic devices | Section 37 Police Crime and Sentencing Act 2022 (UK) | Extraction of Information from electronic devices, typically with agreement of user of the device |
| Maritime powers | Part 4 Chapters 5 (E&W), 6 (S) & 7 (NI) Policing and Crime Act 2017 | Seizure of material pursuant to exercise of maritime law enforcement powers (Designated NCA officer) |
| Other search warrants or statutory seizure powers | Any other seizure power pursuant to a search warrant or statutory search power | Any other seizure power pursuant to a search warrant or statutory search power. For example, powers under the National Security Act 2023. Seek advice from NCA Legal if necessary to confirm whether the power means that BPD authorisation is not required per paragraph 3.7 of this Operating Procedure). |
| Money laundering and terrorist financing | | |
| POCA Information Orders | Section 339ZH Proceeds of Crime Act 2002 (UK) | Information order further to a suspicious activity report under Part 7 POCA |
| POCA Suspicious Activity Reports | Part 7 Proceeds of Crime Act 2002 (including a disclosure report under s339ZD POCA | Disclosure to the UKFIU of a reasonable suspicion of money laundering (disclosure not sought by NCA but required by legislation) |
| TACT Information Orders | Section 22B Terrorism Act (UK) | Information order further to a disclosure of a reasonable suspicion of terrorist financing (Judge) |
| TACT Suspicious Activity Reports | Part III Terrorism Act 2000 (UK) | Disclosure to the UKFIU of a reasonable suspicion of terrorist financing (disclosure not sought by NCA but required by legislation) |

| | | |
|---|---|---|
| Information obtained by UKFIU on behalf of or from foreign FIUs | Schedule 6A Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (UK) | Information obtained by UK Financial Intelligence Unit on behalf of or from foreign FIUs |
| Information from legal proceedings | | |
| Information provided in defence of criminal proceedings | Part 1 Criminal Procedure and Investigations Act 1996 (E&W, NI)<br>Part 6 Criminal Justice and Licensing Act (Scotland) Act 2010 | Information provided in defence of criminal proceedings |
| Information provided in defence of confiscation proceedings | Part 2 (E&W)<br>Part 3 (Scotland)<br>Part 4 (NI)<br>Proceeds of Crime Act 2002 | Information provided in defence of confiscation proceedings |
| Information provided in defence of other POCA proceedings | Part 5<br>Proceeds of Crime Act 2002 (UK) | Information provided in defence of civil recovery or cash / listed asset / bank account forfeiture proceedings |
| Information provided in defence of Revenue proceedings | Part 6<br>Proceeds of Crime Act 2002 (UK) | Information provided in defence of Revenue proceedings |
| Information provided in relation to | Part 1<br>Serious Crime Act 2007 (UK) | Information provided in respect of litigation or compliance with Serious Crime Prevention Orders |
| Information provided in relation to SROs / SHPOs etc | Part 2<br>Sexual Offences Act 2003 (UK) | Information provided in respect of litigation or compliance with orders under Part 2 of the Sexual Offences Act 2003, such as Sexual Risk Orders and Sexual Harm Prevention Orders |
| Information provided in relation to other legal proceedings | (Various) Court / Tribunal Procedure Rules (UK) | Information provided in relation to other legal proceedings further to court procedure rules (for example, but not restricted to, information provided pursuant to Civil Procedure Rules, Magistrates' Court Rules, Criminal Procedure Rules, or tribunal procedure rules) |
| Investigatory Powers | | |
| Part 3 Property Interference | Section 93(1)<br>Police Act 1997 (UK) | Information obtained pursuant to an authorisation for interference with property or wireless telegraphy<br>(Deputy Director NCA) |
| Directed or Intrusive Surveillance Authority (DSA / ISA) | Part 2 Regulation of Investigatory Powers Act 2000 (UK)<br>Regulation of Investigatory Powers (Scotland) Act 2000 | Covert surveillance obtaining, for the purposes of a specific investigation or operation, private information about a person. |

| | | |
|---|---|---|
| Covert Human Intelligence Source (CHIS) | Part 2 Regulation of Investigatory Powers Act 2000 (UK)<br>Regulation of Investigatory Powers (Scotland) Act 2000 | Information obtained pursuant to a covert human intelligence source authorisation (including undercover officers as 'relevant sources') |
| Interception | Part 2 Investigatory Powers Act 2016 | Interception, in the course of transmission by means of postal service or telecommunications system, of |
| Communications Data | Part 3 Investigatory Powers Act 2016 (UK) | Obtaining communications data for the purposes of a specific investigation or operation. |
| Equipment Interference | Part 5 Investigatory Powers Act 2016 (UK) | Obtaining communications, equipment data, or any other information |
| Overseas production order | Section 1 Crime (Overseas Production Order) Act 2019 | Obtaining electronic data from designated overseas country |
| Powers relating to overseas investigations | | |
| CICA Warrant / Production Order | Section 17(4) and 22(1),(4) (E&W, NI) / Section 18(1) and 22(1) (Scotland) Crime (International Co- Operation) Act 2003 | Seizure of evidence following a warrant / production order made in relation to an overseas criminal investigation (varies depending on the power used – Justice of the Peace / Sheriff or Judge) |
| Extradition Warrants and Seizure Powers | Part 4 Extradition Act 2003 (UK) | Seizure of relevant material relating to extradition (varies depending on the power used – from Designated NCA Officer to Judge) |
| Orders relating to POCA External Investigations | Proceeds of Crime Act 2002 (External Investigations) Orders 2013 and 2014 (UK) / Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005 | Orders relating to seizure of material and obtaining material further to an external investigation under the Proceeds of Crime Act 2002 (Judge) |
| Immigration and Customs Powers | | |
| Immigration Warrants and Seizure Powers | Part III Immigration Act 1971 (UK) | Seizure of evidence relating to immigration offences (varies depending on the power used – from Designated NCA Officer to Justice of the Peace) |
| Seizure of electronic devices | Schedule 2 Illegal Migration Act 2023 | Seizure of electronic devices used by illegal migrants (Designated NCA Officer) |
| Customs detention of anything liable to forfeiture | Section 139 Customs and Excise Management Act 1979 | Detention of anything liable to forfeiture under the Customs and Excise Management Act 1979 (Designated NCA Officer) |
| Customs search warrant | Section 161A Customs and Excise Management Act 1979 | Search warrant for anything liable to forfeiture under the Customs and Excise Management Act 1979 (Justice of the Peace) |
| Other powers | | |
| CSEA Material reported to NCA | Section 66 Online Safety Act 2023 | Child Sexual Exploitation and Abuse material reported to the NCA pursuant to the requirement under the Online Safety Act |

| | | |
|---|---|---|
| Taxpayer and Third-Party Notices | Part 1 of Schedule 36 Finance Act 2008 (UK) | Notice requiring information from a taxpayer or third parties pursuant to proceedings under Part 6 Proceeds of Crime Act 2002 |
| Powers to inspect premises and remove documents | Part 2 and 3 of Schedule 36 Finance Act 2008 (UK) | Power to inspect business premises (including involved third parties) and remove/take copies of documents |
| Chemical Suspicious Activity Reports | Article 9 of Council Regulation (EC) No. 111/2005, in conjunction with Regulation 3 of SI 2008/296; and Article 8 of Regulation (EC) No. 273/2004 of the European Parliament and of the Council, in conjunction with Regulation 3 of SI 2008/295 (UK) | Disclosure to NCA Chemical Control Team by operators of any circumstances, such as unusual orders or transactions, which suggest that specified drug precursors might be diverted for the illicit manufacture of narcotic drugs or psychotropic substances (disclosure not sought by NCA but required by legislation) |
| Passenger Name Records | Immigration and Police (Passenger, Crew and Service Information) Order 2008, in conjunction with, Section 32 Immigration, Asylum and Nationality Act 2006 (UK) | Requirement on owner or agent of a ship or aircraft to comply with a requirement to provide passenger or service information |

[i] [i] References to legislative provisions includes those provisions as modified by statutory instruments. For example, the Police and Criminal Evidence Act 1984 has been modified, in particular, by the Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013/1542; the Crime and Courts Act 2013 (Application and Modification of Certain Enactments) Order 2014/1704; the Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015/1783; and the Crime and Courts Act 2013 (Application and Modification of Certain Enactments) Order 2016/1143.

[ii] This provision applies in England and Wales only. This list of commonly used powers includes equivalent provisions provided for in Northern Ireland and Scotland: in Northern Ireland by Article 10(2) of the Police and Criminal Evidence (Northern Ireland) Order 1989/1341; and in Scotland under a warrant obtained under common law (see Section 46 of the Criminal Justice (Scotland) Act 2016) or Section 23E of the Criminal Law (Consolidation) (Scotland) Act 1995.

[iii] This provision applies in England and Wales only. This list of commonly used powers includes equivalent provisions provided for in Northern Ireland and Scotland: in Northern Ireland by Article 20(2) of the Police and Criminal Evidence (Northern Ireland) Order 1989/1341; and in Scotland under common law (see Section 46 of the Criminal Justice (Scotland) Act 2016).

[iv] This provision applies in England and Wales only. This list of commonly used powers includes equivalent provisions provided for in Northern Ireland and Scotland: in Northern Ireland by Article 21(2)-(4) of the Police and Criminal Evidence (Northern Ireland) Order 1989/1341; and in Scotland under common law (see Section 46 of the Criminal Justice (Scotland) Act 2016).

[v] This provision applies in England and Wales only. This list of commonly used powers includes equivalent provisions provided for in Northern Ireland and Scotland: in Northern Ireland by Article 22(1) of the Police and Criminal Evidence (Northern Ireland) Order 1989/1341; and in Scotland under common law (see Section 46 of the Criminal Justice (Scotland) Act 2016).

[vi] This provision applies in England and Wales only. This list of commonly used powers includes equivalent provisions provided for in Northern Ireland and Scotland: in Northern Ireland by Article 34(9) of the Police and Criminal Evidence (Northern Ireland) Order 1989/1341; and in Scotland under common law (see Sections 47 and 48 of the Criminal Justice (Scotland) Act 2016).

[vii] This provision applies in England and Wales only. This list of commonly used powers includes equivalent provisions provided for in Northern Ireland and Scotland: in Northern Ireland by Schedule 1 paragraph 4, in conjunction with Article 9, of the Police and Criminal Evidence (Northern Ireland) Order 1989/1341; and in Scotland under a warrant or production order obtained under common law (see Section 46 of the Criminal Justice (Scotland) Act 2016) or Section 23B of the Criminal Law (Consolidation) (Scotland) Act 1995.

[viii] This provision applies in England and Wales only. This list of commonly used powers includes equivalent provisions provided for in Northern Ireland and Scotland: in Northern Ireland by Schedule 1 paragraph 10, in conjunction with Article 9 of the Police and Criminal Evidence (Northern Ireland) Order 1989/1341; and in Scotland under a warrant obtained under common law (see Section 46 of the Criminal Justice (Scotland) Act 2016) or Section 23E of the Criminal Law (Consolidation) (Scotland) Act 1995.