Counter Fraud Authority

I2 Analyst's Notebook including geographical mapping (i2 Analyst's Notebook Connector for Esri) – Geographical mapping

Data Protection Impact Assessment

July 2026

V1

NHS fraud.
Spot it. Report it.
Together we stop it.

Executive Summary

This document contains information in relation to I*2 Analyst's Notebook (ANB)*

The document is deemed OFFICIAL and any information viewed/obtained within it should be treated in the appropriate manner as advised and set out in the Government Security Classifications (June 2023).

More information in relation to this data classification, including the requirements for working with these assets can be found here:

Government Security Classifications Policy June 2023.docx (publishing.service.gov.uk)

In particular please note that:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level. There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

Nothing contained herein should be construed as endorsing any particular Technical Solution to any United Kingdom Government Invitation to Tender.

Table of contents

Executive Summary **2**

Links & Dependencies **5**

1. Data Protection Impact Assessment Requirement & Process **6**

Introduction 6

I2 ANB - General Description 7

Data Protection Impact Assessment 7

Ownership ..... **Error! Bookmark not defined.**

2. DPIA Report **21**

Section 1: Data Maintenance and Protection Overview 21

Section 2: Uses of the Application and the Data 21

Section 3: Data Retention 22

Section 4: Internal Sharing and Disclosure of Data 22

Section 5: External Sharing and Disclosure of Data 22

Section 6: Notice/Signage 22

Section 7: Rights of Individuals to Access, Redress and Correct Data 22

Section 8: Technical Access and Security 23

Section 9: Technology 23

3. Compliance Checks **23**

DPA 2018 Compliance Check 23

The Privacy and Electronic Communications Regulations 23

The Human Rights Act 24

The Freedom of Information Act 24

Conclusion 24

Annex A - Definition of Protected Personal Data **25**

Annex B - Data Protection Compliance Check Sheet ..... Error! Bookmark not defined.

Prefix	
Reference:	**DPIA** (I2 ANB + mapping**)**
Date:	**05/08/2026**
Version:	**1**
Supersedes	**N/A**

Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	2018	HMG
EU GDPR	EU General Data Protection Regulation	All	2016	GDPR
FOI	Freedom of Information Act	All	2000	HMG
Government Security Classifications	Government Security Classifications	All	June 2023	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

1. Data Protection Impact Assessment Requirement & Process

Introduction

1. The General Data Protection Regulation (GDPR) 2016 introduces a new obligation to undertake Data Protection Impact Assessments (DPIAs), before carrying out types of processing **'likely to result in high risk(s) to individuals' interests'**. DPIAs are now mandatory for certain types of processing and there are specific legal requirements for content and process. Where a DPIA identifies a 'high risk' that cannot be mitigated, the Information Commissioner's Office (ICO) must be consulted.
2. DPIAs provide a way to systematically and comprehensively analyse the intended processing and help to identify and minimise data protection risks. In addition to considering compliance risks, they should also consider broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals or to society at large, whether it is physical, material or non-material.

3. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It does not have to eradicate the risks altogether, but should help to minimise them and assess whether or not remaining risks are justified. A DPIA may cover a single processing operation or a group of similar processing operations. For new technologies you may be able to use a DPIA done by the product developer to inform your own DPIA on your implementation plans.

4. A DPIA must consider 'risks to the rights and freedoms of natural persons'. While this includes risks to privacy and data protection rights, it can also affect other fundamental rights and interests:

    a. "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead **to physical, material or non-material damage**, in particular: where the processing **may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy**, **unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage**; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data[1]…"

5. Under GDPR you must carry out a DPIA where for example you plan to:

    a. process special category or criminal offence data on a large scale.

6. The ICO also requires a DPIA to be undertaken for example, where you plan to:

    a. use new technologies;

    b. match data or combine datasets from different sources;

    c. collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

7. DPIAs are an essential part of the organisation's accountability obligations under GDPR and an integral part of the 'data protection by default and design approach'. An effective DPIA helps to identify and fix problems at an early stage, demonstrate compliance with data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.
8. Conducting a DPIA is a legal requirement for any type of processing. Failure to carry out a DPIA in required cases may leave the organisation open to enforcement action, including a **fine of up to €10 million**.

[1] GDPR - Recital 75

9. This DPIA is related to the NHSCFA Risk Assessments, which outline the threats and risks. The Risk Assessment document was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.
10.

I2 ANB + mapping - General Description

11. I2 Analyst's Notebook is described as 'visual analysis capabilities that quickly turn complex sets of disparate information into high-quality, actionable intelligence to help them and those involved in intelligence analysis identify, predict, and counter criminal, terrorist and fraudulent activities.' i2 Analyst's Notebook - Discover and deliver actionable intelligence | i2

12. I2 Insights is an add-on for I2 ANB meant to speed up data preparation and reduce processing errors, it also includes a basic form of mapping i2 Insights

13. *'i2 Analyst's Notebook Connector for Esri adds geospatial analysis to the capabilities of i2 Analyst's Notebook'* Welcome to i2 Analyst's Notebook Connector for Esri. ArcGIS has an up to date mapping software as part of the package, which supports latitude and longitude. REDACTED most prevalently the tool used for mapping geographical coordinates.

14. ArcGIS Enterprise is described as a 'self-hosted geographic information system (GIS) software for mapping, analytics, and data management. It runs on your infrastructure to meet compliance, security, and customization needs'. Enterprise GIS System | Cloud-Native Geospatial Software | ArcGIS Enterprise includes comprehensive mapping to help with critical decision making.

15. REDACTED

16. This is the first DPIA to be completed on the I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise, however a previous DPIA has been produced for ArcGIS Esri via PowerBI and a PIA on IBASE. This DPIA has been carried out by the Information Governance Officer, in consultation with Strategic Intelligence Lead and the Information Governance and Risk Management Lead.

17. I2 ANB in addition to GDPR is also required to comply with other relevant HMG legislation including where applicable with Data Protection laws. Also, *'Esri supports alignment with the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and has a Data Processing Addendum (DPA) containing Standard Contractual Clauses available within the ArcGIS Trust Center documents that customers can sign. Lastly, HIPAA eligible services are available for ArcGIS Online, which are backed by a Business Associate Agreement (BAA).'* *Esri Software Security and Privacy - SDLC*

Data Protection Impact Assessment

18. To ensure the I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a DPIA. This DPIA is based on the ICO's recommended template[2] comprised of seven steps:

    Step 1 - Identify the need for a DPIA

[2] Version 0.3 (20180209)

Step 2 - Describe the processing

Step 3 - Consultation process

Step 4 - Assess necessity and proportionality

Step 5 - Identify and assess risks

Step 6 - Identify measures to reduce risk

Step 7 - Sign off and record outcomes

STEP 1: Identify the need for a DPIA

Explain broadly what the system/project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

eed for a DPIA has been identified to ensure that it is appropriate to continue use of I2 Analyst's Notebook for charts and maps for intelligence and evidential purposesDATA REDACTED.

Because personal data could potentially be at risk due to the source of data (Ibase, CLUE and evidential exhibits) containing sensitive information relating to allegations, intelligence and investigations / operations this DPIA has been produced to confirm any personal /person identifiable data is secure when using this software, for any associated risks to be identified and then mitigated effectively in advance of use.

A REDACTED

In addition to its regular charting use, I2 ANB can also be used to access ArcGIS Esri including ArcGIS Enterprise. '*i2 Analyst's Notebook Connector for Esri adds geospatial analysis to the capabilities of i2 Analyst's Notebook. It fully integrates with ArcGIS Server geospatial functions, which means that you can conduct association, temporal, and geospatial analysis in a single work environment.*' - *Welcome to i2 Analyst's Notebook Connector for Esri*

A REDACTED

Therefore, I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise, have been identified as a potential option, it creates no extra costs or requirement for licences. It has been discussed with the I2 group directly and they have kindly provided information on what is already part of the NHSCFA contract, as well as installation and organisation of a bespoke training day.

A REDACTED

Therefore, research has been undertaken to understand how I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise hold or process the data supplied. What is understood and would be beneficial to be further assessed by yourselves is whether we can use I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise.

The information in response to step 4 – question 8 - would suggest that only coordinates and addresses are passed to ESRI from I2 ANB if you already have latitude and longitude to input, which is the case A REDACTED.

https://doc.arcgis.com/en/microsoft-365/latest/power-bi/faqs.htm#:~:text=The%20ArcGIS%20for%20Power%20BI%20visual%20was%20designed%20to%20protect,and%20compliance%20for%20additional%20information.

STEP 2: Describe the processing

Describe the nature of the processing:

1. How will you collect, use, store and delete data?
   -extract or provided
   -Intelligence unit only folders
   -data retention schedule / policy

2. What is the source of the data?

3. Will you be sharing data with anyone (consider using a flow diagram or other way of describing data flow)?

4. Why types of processing identified as 'likely high risk' are involved?

1. **How will you collect, use, store and delete data?**

DATA REDACTED.

2. **What is the source of the data?**

DATA REDACTED

3. Will you be sharing data with anyone?

DATA REDACTED

4. **What types of processing identified as likely high risk are involved?**

DATA REDACTED

Describe the scope of the processing:

1. What is the nature of the data and does it include special category or criminal offence data?

2. How much data will you be collecting and using?

3. How often?

4. How long will you keep it?

5. How many individuals are affected?

6. What geographical area does it cover?

1. **What is the nature of the data and does it include criminal offence data?** Allegations and investigations. Yes, it does contain / come under criminal offence data.

20. **How much data will you be collecting and using?** Lines of data for allegations and investigations can often have 100's or 1000's rows in excel.

21. **How often?** Quarterly, annually and when investigations support requests are made, or assessments are commissioned.

22. **How long will you keep it?** Data would be reviewed and redacted / anonymised or deleted in accordance with SITs data retention SOP. V1 NHSCFA SIT Data Retention SOP Final 240524.docx

23. **How many individuals are affected?** It will affect the number of data subjects who are subjects of intelligence gathering and investigations. So, the number is unknown.

2. **What geographical areas does it cover?** The geographical area we map covers England and sometimes mapping coordinates globally. The mapping would be conducted where staff work / at their office base / home on NHSCFA laptops or phones. '*Analyst's Notebook Connector for Esri is able to connect to any ArcGIS server'* Welcome to i2 Analyst's Notebook Connector for Esri and Esri servers are based in US, but personal identifiable data is stored by the end user in an i2 proprietary file type (.anb) which can only be opened using i2 applications, those being: Analyst's Notebook and Chart Reader. Only coordinates and addresses are then passed to ArcGIS Esri. Reference to slide 7 of : ArcGIS Online: Compliance and Security ' ArcGIS data is hosted within AWS and MS Azure data centres in US by default' But the slide goes on to explain: new organisations can choose to have their data stored in regions outside the US, such as EU or AP regions'. Data is also encrypted at rest and in transit with HTTPS w/TLS for in-transit and AES-256 at rest. Privacy assurance is in place as even ArcGIS online is both GDPR and CCPA aligned. Also, there is a contact email for Esri's software security and privacy team for questions or concerns SoftwareSecuirty@Esri.com. *'i2 intelligence analysis product portfolio of IBM, including the i2 Analyst's Notebook, i2 Enterprise Insight Analysis (EIA) and i2 iBase platforms'* Harris Acquires i2 Product Portfolio from IBM are owned by N. Harris Computer Corporation (Harris), owned by Constellation Software Inc which is registered in Canada.

Describe the context of the processing:

1. What is the nature of your relationship with the individuals?

2. How much control will they have?

3. Would they expect you to use their data in this way

4. Do they include children or other vulnerable groups?

5. Are there any prior concerns over this type of processing or security flaws?

6. Is it novel in any way?

7. What is the current state to technology in this area?

8. Are they any current issues of public concern that you should factor in?

9. Are you signed up to any approved code of conduct or certification scheme (once any are approved)?

24. **Nature of your relationship with the individuals =** DATA REDACTED The NHSCFA recognises the sensitive nature of this information and takes significant measures to protect the privacy and confidentiality of individuals involved in fraud investigations and cases. Strict access controls, encryption, and other security measures are in place to ensure that only authorised personnel have access to this data for lawful investigative purposes. The processing of such personal data within I2 ANB, ArcGIS Esri and Insight is carried out in compliance with relevant data protection regulations and guidelines to safeguard the privacy rights of individuals involved in fraud investigations and cases. DATA REDACTED.

1. **How much control will they have?** For individuals involved in ongoing and completed fraud investigations and cases, control over their data may be subject to legal and operational restrictions. To maintain the integrity of investigations and protect the privacy of all parties involved, certain limitations may apply to their ability to directly modify or delete their data the NHSCFA store and process within the I2 ANB system and the systems it hosts such as ARCGIS Esri and Insight. However, the NHSCFA ensures that individuals' rights are respected and that appropriate measures are in place to handle their data securely and confidentially. The NHSCFA is committed to promoting transparency and providing individuals with a reasonable degree of control over their data within the bounds of legal and operational requirements. Measures are in place (Privacy Notice) to inform individuals about their rights, enable them to exercise those rights where applicable, and address any concerns.

2. **Would they expect you to use their data in this** way? Individuals report to the NHSCFA with the intention of notifying us about an alleged offence, therefore it would be expected that this data would be used to combat fraud. In the case of individuals involved in ongoing and completed fraud investigations and cases, they would reasonably expect their data to be used for investigative purposes, intelligence analysis. Given the NHSCFA's role as the national investigative/prevention body for fraud within the NHS, individuals involved in such cases understand that the processing of their data is necessary to fulfil the NHSCFA's statutory responsibilities and to support the overall integrity of the investigative process. Privacy notices and appropriate consent mechanisms are implemented to ensure that individuals are well-informed about the purposes for which their data will be used and to provide them with the opportunity to express their preferences and exercise their rights related to data processing. There exists an imbalance between the data controller and data subjects where allegations are reported against a subject. As this is invisible processing of personal data subjects are unaware of their subject rights.

25. **Do they include children or other vulnerable groups?** Potentially, if you are named in an allegation or have committed an offence, you would likely expect that law enforcement or similar to process your data with the intent to investigate, possibly going on to prosecute, Especially, if you are a defendant in court, because the prosecution's evidence is being disclosed to you under disclosure for CPS. Individuals who report to us would be aware that they are reporting with the intention to reduce / mitigate / decrease fraud. When reporting to the NHSCFA there is a page which describes: How will your information be used? | Report Fraud | NHSCFA and the first paragraph states ‘for the purpose of combating fraud and corruption within the NHS’.

5. **Are there any prior concerns for this type of processing or security flaws?** No. The NHSCFA recognises the importance of addressing any prior concerns and security flaws relating to the processing of data in relation to I2 ANB, ArcGIS Esri and Insight, as the organisation has its own PIA that covers the processing of data in Ibase within NHS-Protect_PIA-iBase.pdf, as well as a DPIA within Data_Protection_Impact_Assessment_ArcGIS_Esri_for_Power_BI.pdf in which ARCGIS Esri is hosted by powerBi instead of I2 ANB. This assessment ensures that the data handled within I2 ANB is appropriately protected, and any potential risks are identified and mitigated.

26. **Is it novel in any way?** No, charting and mapping data for strategic, tactical and operational analysis is standard practice across police and other law enforcement bodies which have intelligence units / analysts / researchers.

27. **What is the current state of technology in this area?** Advanced in charting in I2 ANB, however mapping through ARCGIS and insight via I2 ANB we are yet to harness the capabilities for and currently have an inadequate system.

28. **Are there any current issues of public concern?** The charts showing criminal behaviour and money flow etc, as well as the spread of allegations / crime across the country may be picked up in a news cycle if they were leaked into the public domain, however we already produce maps and so do other bodies.

6. **Are you signed up to any approved code of conduct or certification scheme?** The NHSCFA has an ISO ISO27001:2013 certification on information security which covers information processed within the NHSCFA network. *'In 2025, Esri's Information Security Management System (ISMS) was found to be in accordance with ISO 27001:2022 security controls. This includes ArcGIS Online and ArcGIS Location Platform hosted in the European Union (EU) region and physical security controls of US-based operations administration.'* - ISO—ArcGIS Trust Center | Documentation

Describe the purposes of the processing:

1. What do you intend to achieve?

2. What is the intended effect on individuals?

3. What are the benefits of the processing, for you and more broadly?

1. **What do you intend to achieve?** Continued charting capability and improved mapping software, to support intelligence development and investigations.

2. **What is the intended effect on individuals?** Deterring, detecting, investigating and preventing crime to protect all individuals and the NHS. Individuals involved in ongoing and completed fraud investigations and cases benefit from the processing through improved case management & data analysis. The platform's capabilities allow for more effective handling of their data, leading to better investigation outcomes and protection of their rights during the investigative process.

3. **What are the benefits of the processing?** DATA REDACTED. This new software should also help improve intelligence development. This should also improve stakeholder relations as the products they receive will be improved and in line with other public / policing bodies.

STEP 3: Consultation process

Consider how to consult with relevant stakeholders:

1. Describe when and how you will seek individuals' views or justify why it's not appropriate to do so?

2. Who else do you need to involve within your organisation?

3. Do you need to ask your processors to assist?

4. Do you plan to consult information security experts or any other experts?

29. **Describe when and how you will seek individuals' views or justify why not appropriate to do so.** I have also consulted with SIT on the improved mapping software and upcoming training in I2 ANB + mapping, whilst the analysts have all previously completed training in I2 ANB. In certain circumstances seeking individuals' views may compromise ongoing investigations or pose risks to safety. Alternative measures will be implemented to protect confidentiality and privacy.

30. Who else do you need to involve within your organisation? DATA REDACTED

1. **Do you need to ask your processors to assist?** No, it is already a usable system, with no further cost / licences required.

2. **Do you plan to consult information security experts or any other experts?** Information Security experts have been consulted with. They understand that the processing of geo spatial data is carried out in US Esri Servers (AWS & MS-Azure Data Centres), but personal identifiable data is stored by the end user in an i2 proprietary file type (.anb) which can only be opened using i2 applications, those being: Analyst's Notebook and Chart Reader. Only coordinates and addresses are then passed to ArcGIS Esri. Esri then has a strict software security and privacy statement Esri Software Security and Privacy - SDLC. The information security experts have confirmed that this does not create a high risk to any personal data processed.

STEP 4: Assess necessity and proportionality

1. What is your lawful basis for processing?
2. Does the processing actually achieve your purpose?
3. Is there another way to achieve the same outcome?
4. How will you prevent function creep?
5. How will you ensure data quality and data minimisation?
6. What information will you give individuals?
7. How will you help to support their rights?
8. What measures do you take to ensure processors comply?
9. How do you safeguard any international transfers?

1. **What is your lawful basis for processing?** Processing criminal offence data under control of an official authority. To comply with the lawful processing of criminal offence data to ensure the relevant risks have been considered and appropriate safeguards have been identified and meeting broader data protection obligations. Personal data will be processed under GDPR and DPA to perform a task in the public interest or in the exercise of the Authority's official authority.

31. **Does the processing actually achieve your purpose?** Yes, continued use of charting and improved maps for intelligence development and evidential purposes.

32. **Is there any other way to achieve the same outcomes?** No, we procure another charting software or use an inferior one to I2ANB which is industry standard. Also, the current mapping software would need to be revised which has been explored and the solution is accessing ARCGis ESRI through i2 ANB instead of PowerBi.

2. **How will you avoid function creep?** The intention is to use the system for charting and geographical mapping, should any software updates be introduced this is unavoidable. However, any processing of the data which is vastly different to what is declared in this assessment, or different to functions necessary to support the mapping or evidential chain of maps would require a new DPIA which strictly focused on that area.

3. **How will you ensure data quality and data minimisation?** Only collecting and processing relevant data. Also, following data governance and retention policies, providing training on this system, keeping documentation accurate and up to date, encouraging feedback.

4. **What information will you give individuals**? Individuals may exercise their right to access personal data under GDPR. Processing of personal data, how NHSCFA uses it and individual rights are explained in the Authority's privacy notice Privacy Policy | NHS Counter Fraud Authority | NHSCFA.

5. **How will you help support their rights?** With the lawful processing of criminal offence data and compliance with information and access rights in the GDPR and DPA. By providing transparent and easily accessible information on methods to exercise these rights and mechanisms in place to protect personal data.

6. **What measures do you take to ensure processors comply?**

I2 ANB :

How data enters Analyst's Notebook and where is it stored:

- *DATA REDACTED*

i2 Analyst's Notebook Connector for Esri :

What Data is Shared with Esri

- *DATA REDACTED*

33. **How do you safeguard any international transfers**. Requests to share the full data sets behind the maps would have to go through a sharing request / agreement and be authorised by the Data Protection Officer and would be a different process. It appears that i2 ANB data is sorted by the end user in an end file and received only coordinates and addresses are passed to ArcGIS Esri.

STEP 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant, or Severe	**Overall risk** Low, Medium or High
Sharing of data with third parties for commercial gain	Remote	Severe	low
Leakage of products in public eye by those who do not follow protective markings	Possible	Severe	High
Sharing with other service users that exposes where the data originated from (Possibly shared with CPS and possibly disclosed to the defence)	Remote	Severe	Medium
Interference or hacking of I2 ANB / Esri.	Remote	Significant	Low
Inappropriate sharing of personal information.	Remote	Significant	Low
Media outlets picking up the documents for publication and scrutiny	Possible	Significant	Low

STEP 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.	Effect on risk Eliminated, Reduced, Accepted	Residual risk Low, Medium, High	Measure approved by SMT Owner Yes/No
'Sharing of data with third parties for commercial gain' Do not share any products for commercial gain, only for the detection, deterrence, prevention, or prosecution of criminal offences.	Eliminated	Low	YES 05/08/2026
Leaking of products in public eye by those who do not following protective markings and perceived Protective markings and caveats / guidance on handling	Reduced	Medium	YES 05/08/2026
Sharing with other service users that exposes where the data originated form (Possibly shared with CPS and possibly disclosed to the defence.) Protective markings and caveats / guidance on handling.	Accepted	Medium	YES 05/08/2026
'*Interference or hacking of power BI'* It appears that I2 ANB data is sorted by the end user in an and file and received only coordinates and addresses are passed to ArcGIS Esri.	Reduced	Low	YES 05/08/2026
'*Inappropriate sharing of personal information with those who do not have a policing / operational purpose of oversight'* A disciplinary process would follow if actions were intentional to cause disruption. If accidental due to misunderstanding around process, then a lessons learned / training would require completion.	Reduced	Low	YES 05/08/2026
'Media outlets picking up the documents for publication and scrutiny' Protective markings and caveats / guidance on handling. Responding to any contact made from outlets prior to publication with careful consideration.	Reduced	Low	YES 05/08/2026

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by SMT Owner:	05/08/2026	Integrate actions back into project plan, with date and responsibility for completion
Residual risks Approved by SMT Owner:	05/08/2026	If accepting any residual high risk, consult the ICO before proceeding.
DPO advice provided		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice: Having reviewed the DPIA I am satisfied that a comprehensive assessment of the I2 Analyst's Notebook (ANB) platform for mapping personal data and geographical information has been carried out. Strict access controls, encryption, and other security measures are in place to ensure that only authorised personnel have access to this data for lawful investigative purposes. It does not have any direct interconnections with other NHSCFA systems and applications. Access to the platform currently, will be by approximately 8 members of SIT staff, not including database administrators or others in the IIU or wider organisation who use I2 analyst notebook for charting without the mapping capabilities. Which means use will be fully auditable. All data will be held and governed in accordance with current legislative requirements and handled in accordance with organisational best practice and its data retention policy. I am therefore satisfied with the with the organisational security measures employed.		
DPO advice accepted or overruled by:	- 24th July 2026	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' view, you must explain your reasons
Comments:		
This DPIA will be kept under review by the Information and Records Management Officer:		The DPO should also review ongoing compliance with DPIA

2. DPIA Report

Section 1: Data Maintenance and Protection Overview

1. The impact level of I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise was assessed as OFFICIAL and OFFICIAL SENSTIVE (depending on the data supplied for the map) and it can only be accessed / viewed by those approved for dissemination.
2. The following measures briefly describe what controls have been implemented to protect *I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise* and the personal data recorded:
    a. The *I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise will be* accessed by approximately 8 members of staff (SIT) from NHSCFA, unless this team expands further, this estimate does not include the database administrators or others in the IIU or wider organisation who use I2 analyst notebook for charting without the mapping capabilities.
    b. I2 Analyst's Notebook Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise do not have any direct interconnections with other NHSCFA systems and applications as far as I am aware.
    c. The Data Custodian must comply with the data protection requirements Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the NHSCFA register and the NHSCFA DPO is aware of its existence.
3. It is assessed that there are no residual privacy risks to the personal data used by the *I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise.*
4. This DPIA must be reviewed if any changes are made to the personal information if used by the database or any other changes are made that affect the privacy of an individual.

Section 2: Uses of the Application and the Data

5. Who has responsibility for the administration of the *I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise* – the IIU will be mainly using it and Technology team for safety / security.

6. Information in the *I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise* could include; intelligence and evidential sensitive data, including *geographical data.*

7. List identified sensitive:

DATA REDACTED

8. The IAO must comply with data protection requirements. Examples include: regularly reviewing the business requirement to use the personal data; ensuring that the data is not excessive, it is being used for the purpose intended; that there is a deleting and disposal policy; that the application is registered and the DPO is aware of its existence.

Section 3: Data Retention

9. I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise will be subject to NHSCFA Data Handling and Storage Policy. No paper records, but if printed it would be putting into confidential waste bin. Data would be reviewed and redacted or deleted in accordance with SITs data retention SOP.

10. The IAO is required to review the retention period and any requirement to change must be submitted to the Senior Information Risk Owner.

Section 4: Internal Sharing and Disclosure of Data

11. I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise is accessed by approximately 8 members of staff from NHSCFA (SIT) and includes unknown number of database administrators. This estimate does not include the database administrators or others in the IIU or wider organisation who use I2 analyst notebook for charting without the mapping capabilities.

Section 5: External Sharing and Disclosure of Data

12. In some cases information shared with external organisations, would be if it was requested for the administration of justice and the prevention, detection or deterrence of crime. DATA REDACTED

Section 6: Notice/Signage

13. No, allegations are around alleged offences by individuals or multiple people therefore individuals would not be notified that an allegation has been made about them to protect the source. An allegation would in most cases be processed and an investigation commenced first before the subject became aware.

NHSCFA's privacy policy on its website hosts separate sections in relation to data collection, retention and storage. This broadly covers all elements of the NHSCFA usage of data, in a nonspecific manner.

34. Individuals report to the NHSCFA with the intention of notifying us about an alleged offence, therefore it would be expected that this data would be used to combat fraud. The NHSCFA has a webpage How will your information be used? | Report Fraud | NHSCFA when reporting to the NHSCFA. The use of signage or other notifications to notify the public of the gathering and use of personal data is relevant to the *I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise* and therefore not outside the scope of this DPIA. However, the use of this system specifically, is not advertised in the public eye and we do not use the source details. However, the public may become aware of its use when presented in court to jury or if documents were leaked.

Section 7: Rights of Individuals to Access, Redress and Correct Data

15. Individuals subject to certain exemptions, have the right to gain access to their own personal data. In the event an access request is directly or indirectly received by NHSCFA, we are required to provide the individual who has made the request with details of the personal data recorded about them.

16. It is unlikely that many access requests will be received as the personal data recorded is all in relation to alleged criminal offences or criminal offences which are with the CPS or to be submitted to the CPS.

17. In the unlikely event that information is identified as being incorrect, NHSCFA staff will take appropriate steps to correct the record where permissible.

18. All NHS employees and member of the public have the right to access, redress and correct personal data recorded about them.

Section 8: Technical Access and Security

19. The security and technical access architecture of I2 Analyst's Notebook + I2 Insights and Analyst's Notebook Connector for Esri including ArcGIS Enterprise is as explained in this DPIA:

The application and the hosting infrastructure was assessed at **Official-Sensitive and Official** and the hosting infrastructure is subject to the ISO27000 and ISO27001 *[confirm with ISA and amend accordingly]*

20. Access is to systems are restricted to internal staff only.

21. The technical controls to protect the database include: *[confirm with ISA and amend accordingly]*

a. Anti-virus protection;

b. Permission based access controls to shared drive.

c. Logging, audit and monitoring controls.

d. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

22. Analyst's Notebook Connector for Esri including ArcGIS Enterprise should not store personal information and is in ANB I2 desktop app on the NHSCFA system which points to a portal online. Personal identifiable data is stored by the end user in an i2 proprietary file type (.anb) which can only be opened using i2 applications, those being: Analyst's Notebook and Chart Reader.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that Power BI, and the personal data that it records, and its business activities, are compliant and maintain compliance with:

a. The GDPR and the Data Protection Act in general;

b. The Data Protection Principles;

c. The interpretations of the Principles.

2. **This is not a recommendation but a requirement of law.**

3. The roles and responsibilities for the protection of personal data are described in the NHSCFA security policy.

4. The *ArcGIS Esri for Power BI* processes sensitive personal data so a Data Protection Compliance Check Sheet has been completed (see Annex B) describing how the requirements of GDPR and the Data Protection Act 2018 have been complied with, See; also Annex A Category C *[delete / amend accordingly]*

The Privacy and Electronic Communications Regulations

5. The Privacy and Electronic Communications Regulations is not applicable as personal data is not exchanged with external organisations for commercial purposes.

The Human Rights Act

6. The decisions and activities of the organisation are undertaken in compliance with the Human Rights Act, having due regard to appropriateness and proportionality to ensure compatibility with Convention rights.

The Freedom of Information Act

7. As a public authority we are compliant with the provisions of the Freedom of Information Act, in proactively publishing and making available upon request, certain recorded information held by the organisation subject to any relevant exemption(s). However, no personal information would be disclosed under the Freedom of Information Act as this would breach the data protection principles.

Conclusion

8. There are no residual privacy risks to the personal data recorded in the *ArcGIS Esri for Power BI*. The controls described in this DPIA explain in detail how the data is protected and managed in accordance with the GDPR and Data Protection Act 2018. The DPO is responsible for ensuring that the controls are implemented through the life cycle of the system.

Annex A - Definition of Protected Personal Data

Personal data includes all data falling into Categories A, B or C below:-

A. Information that can be used to identify a living person, including:

Name;
Address;
Date of birth;
Telephone number;
Photograph, etc.

Note: this is not an exhaustive list.

B. Information which, if subject to unauthorised release, could cause harm or distress to an individual, including:

Financial details e.g. bank account or credit card details;
National Insurance number;
Passport number;
Tax, benefit or pension records;
DNA or fingerprints;
Travel details (for example, at immigration control or oyster records);
Place of work;
School attendance/records;
Material related to social services (including child protection) or housing casework.

Note: this is not an exhaustive list.

C. Sensitive personal data relating to an identifiable living individual, consisting of:

Racial or ethnic origin;
Political opinions;
Religious or other beliefs;
Trade union membership;
Physical or mental health or condition;
Sexual life
Commission or alleged commission of offences;
Proceedings relating to an actual or alleged offence.

Any data set containing this information must be processed in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018).

Particular care must be taken with data in Category B and with any large data set. Information on smaller numbers of individuals may justify additional protection because of the nature of the individuals, source of the information, or extent of information.

There are additional, specific constraints within the provisions of GDPR and the DPA (2018) on the processing of data in Category C.