NHS Counter Fraud Authority

Microsoft Power Platform & Dataverse

Data Protection Impact Assessment

July 2023

V1.1 Published

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

Executive Summary

The purpose of conducting a Data Protection Impact Assessment (DPIA) for Microsoft's Power Platform is to assess and mitigate privacy risks associated with the platform's data processing activities. Power Platform is a suite of cloud-based services and tools that enables the NHSCFA to create and manage business applications, workflows, and data analytics. It consists of four key components: Power Apps, Power Automate, Power BI, and Power Virtual Agents. As Power Platform involves the processing of personal data, conducting a DPIA ensures compliance with data protection regulations and helps identify and address potential privacy risks.

This document is deemed OFFICIAL, and any information viewed/obtained within this document 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)

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.'**

The document is subject to CROWN COPYRIGHT. It is provided with confidence under existing laws, regulations and agreements relating to the protection of data and shall be so protected. The information contained herein is proprietary and shall only be used for the purposes intended at release. It shall not be reproduced, adapted, or used in, whole or in part, for any other purpose without the prior written consent of the Secretary of State for DEPT in the Government of the United Kingdom.

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

Table of contents

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Web Application Development Specialist	DPIA / Microsoft Power Platform & Dataverse	DPO	V0.1	05.06.23	Initial creation
Reviewed by Head of Business Support	DPIA / Microsoft Power Platform & Dataverse	DPO	V1.0	28.7.23	Approved.
Reviewed by Head of Business Support	DPIA / Microsoft Power Platform & Dataverse	DPO	V1.1	28.7.23	Page 34 requirements annotated & DPIA Approved.

Prefix	
Reference:	**DPIA Microsoft Power Platform & Dataverse**
Date:	**July 2023**
Author:	**Web Application Development Specialist**
Data Owner:	**NHSCFA**
Version:	**1.1**
Supersedes	**NA**

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

- 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.

- 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.

- 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.

- 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]…"

- 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.

- 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');

- 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.

- 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

- 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.

Microsoft Power Platform & Dataverse General Description

- Power Platform is a suite of cloud-based services and tools that enable organisations to create and manage business applications, workflows, and data analytics. It consists of four key components: Power Apps, Power Automate, Power BI, and Power Virtual Agents. As Power Platform involves the processing of personal data, conducting a DPIA ensures compliance with data protection regulations and helps identify and address potential privacy risks.

- Power Apps is a component of Power Platform that allows the NHSCFA to build custom applications without extensive coding knowledge. These applications often involve the collection and processing of personal data, making it essential to conduct a DPIA to assess the privacy implications.
- Power Automate, another component, enables the creation of automated workflows to streamline business processes. It involves the transfer and manipulation of data, which may include personal information, emphasising the need for a DPIA to identify and mitigate associated risks.
- Power BI is a powerful business intelligence and data visualisation tool within Power Platform. It enables organisations to analyse and present data in a user-friendly manner. As data analysis often involves personal data, conducting a DPIA is crucial to assess the potential impact on data subjects' rights and freedoms.
- Power Virtual Agents, the fourth component, allows the creation of AI-powered chatbots to automate customer interactions. This involves processing personal data, such as customer inquiries or support requests, necessitating a DPIA to ensure privacy compliance and protect individuals' privacy.

Dataverse

- Dataverse is a cloud-based data storage and management service provided by Microsoft. It serves as a foundational component of the Power Platform suite, offering a secure and scalable environment to store, organise, and share data. Dataverse provides a structured and relational database, enabling users to create tables, define relationships, and enforce data integrity rules. It supports the storage of various data types, including PII, and offers a range of features for data manipulation, integration, and collaboration.
- Power Platform utilises Dataverse as a primary data storage solution across its components, including Power Apps, Power Automate, Power BI, and Power Virtual Agents. Each component interacts with Dataverse to store and retrieve data, creating a cohesive ecosystem for building business applications and automating processes.
- Power Apps leverages Dataverse as the underlying data source, enabling NHSCFA developers to define tables, fields, and relationships directly within the application builder. Power Apps utilises Dataverse's data access capabilities to read, write, and update data in real-time, making it a robust platform for building data-driven applications.
- Power Automate integrates with Dataverse to trigger actions and manipulate data stored within tables. Workflows can be designed to retrieve, update, or create records in Dataverse, allowing for seamless data processing and synchronisation across various systems and applications.
- Power BI connects directly to Dataverse as a data source, allowing NHSCFA analysts to build rich and interactive reports and dashboards. Power BI leverages Dataverse's capabilities to retrieve large volumes of data, perform complex calculations, and visualise insights, empowering organisations to make data-driven decisions.
- Power Virtual Agents utilises Dataverse to store and retrieve data, enabling the chatbot to provide personalised responses based on the user's information. Dataverse integration within Power Virtual Agents ensures seamless access to relevant data, improving the chatbot's effectiveness and enhancing the overall user experience.

Power Platform Security

- Power Platform offers a comprehensive set of security features to safeguard data and protect the integrity of the platform. The platform leverages various security mechanisms to control access, authenticate users, and enforce data protection policies.
- Active Directory (AD) plays a crucial role in Power Platform security. AD is Microsoft's identity and access management solution, providing a centralised directory of users, groups, and security policies. Power Platform integrates with AD to manage user authentication and authorisation, ensuring that only authorised individuals can access and interact with the platform and its components.
- Power Platform offers a range of features to customise and configure security roles according to specific business needs. These features include:
- Entity-Level Permissions: Administrators can grant or deny access to specific entities (tables) within the platform, ensuring that users can only interact with relevant data based on their roles.
- Field-Level Security: Organisations can implement field-level security to restrict access to specific fields within entities, allowing fine-grained control over sensitive data.
- Business Process Flows: Security roles can be configured to control access to specific stages or steps within business process flows, ensuring compliance and data integrity.
- Model-Driven Apps and Canvas Apps: Security roles can be tailored to define access rights to model-driven apps (built on the Common Data Service) and canvas apps, ensuring that users only see and interact with the appropriate applications and functionalities.
- Custom Entities and Web Resources: Administrators can extend the security model to include custom entities and web resources, providing granular control over custom-developed components and data.
- Through proper authentication, role-based access control, and customisation of security roles, organisations can effectively protect data, prevent unauthorised access, and maintain data integrity within their Power Platform deployments. By following the best practices and configuring security roles to align with business requirements, the NHSCFA can confidently leverage the power of Power Platform while maintaining a secure and trusted environment.

Data Integration

- The Power Platform provides robust data integration capabilities, allowing seamless connectivity and collaboration with various NHSCFA applications. This includes integration with applications such as CPOD, LBS, the Public website, and the Fraud Manual, as well as third-party solutions like iBase, CLUE, ESR, and Go2. Each of these applications has its own independent Data Protection Impact Assessment (DPIA), which is publicly available on the NHSCFA's website, ensuring transparency and compliance with data protection regulations.
- The Power Platform integrates with NHSCFA applications to facilitate efficient data exchange, streamline case management processes, enhance fraud prevention efforts, and improve analytical capabilities. It enables the Power Platform to access relevant data, update fraud prevention guidelines, and support online reporting and secure information capture through integration with the NHSCFA's Public website. Additionally, the Power Platform collaborates with third-party solutions such as iBase and CLUE to enhance fraud analysis, investigation, and knowledge management.
- The Power Platform integrates seamlessly with Microsoft services, including Office 365, Teams, SharePoint, OneDrive, and Outlook. This integration allows users to leverage familiar tools for document management, collaboration, communication, and workflow automation within the NHSCFA. It enhances productivity, promotes efficient data sharing, and facilitates real-time collaboration among team members.
- The integration of the Power Platform with NHSCFA applications and Microsoft services is aimed at improving data management, analytical capabilities, fraud detection, and prevention efforts. It enables a comprehensive and integrated approach to fraud management, leveraging the strengths of different applications and services while adhering to data protection and privacy regulations.

Power Platform Environments

- The Platforms data models and processes are segregated into three distinct environments to ensure data integrity, security, and optimised workflows within each specific area. The Central, Inteliverse, and HUB environments cater to the unique requirements of workforce management, operational data handling, and stakeholder engagement, respectively. This segregation promotes efficiency, data privacy, and compliance with relevant regulations.

- The Central environment within the Power Platform is designed to handle workforce and employee management, as well as employee engagement activities. It provides functionalities for managing employee data, such as HR records, skills, performance evaluations, and training. Additionally, it facilitates employee engagement initiatives, such as surveys, feedback mechanisms, and communication channels. The Central environment ensures effective workforce management, promotes employee satisfaction, and enhances overall organisational performance.
- The Inteliverse environment within the Power Platform is dedicated to handling operational data, including intelligence and case management data. This environment supports fraud detection, investigation, and prevention efforts by integrating various data sources and providing analytical capabilities. It enables efficient case management, data analysis, and intelligence sharing among authorised users. The Inteliverse environment enhances the NHSCFA's ability to identify fraud patterns, improve investigations, and collaborate effectively across teams.
- The HUB environment is designed to handle NHS organisational data and stakeholder engagement. It incorporates a Customer Relationship Management (CRM) system built on PowerApps and Dataverse. This environment enables the NHSCFA to manage interactions with NHS organisations, stakeholders including nominated fraud personnel, and other partners the NHSCFA engage with. It supports relationship management, tracks communication history, and facilitates engagement activities. The HUB environment enhances stakeholder collaboration, ensures effective communication, and strengthens relationships with key entities in the healthcare sector.

Data Protection Impact Assessment

- This is the only DPIA to be completed on Microsoft Power Platform & Dataverse and it has been carried out by the Information and Records Management Officer, in consultation with the Web Application Development Specialist and the Information Governance and Risk Management Lead.

- The platform, in addition to GDPR, is also required to comply with other relevant HMG legislation including where applicable the Data Protection Act 2018, Human Rights Act 1998 and Freedom of Information Act 2000.
- To ensure the platform 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.

- 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.

[2] Version 0.3 (20180209)

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 to or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The system/project aims to achieve efficient data management, streamlined processes, and enhanced collaboration within the NHSCFA through the implementation of the Power Platform. The Power Platform comprises three main environments that segregate different data models and processes: Central, Inteliverse, and the HUB.

The segregation of data models and processes into the Central, Inteliverse, and HUB environments within the Power Platform necessitates a thorough DPIA to justify the need for privacy considerations and safeguards. Conducting a DPIA enables the NHSCFA to assess and mitigate potential risks associated with the processing of personal data within each environment.

Given the nature of the Central environment, which handles workforce and employee management, it involves sensitive personal data, including HR records, performance evaluations, and training information. Conducting a DPIA ensures that appropriate security measures, access controls, and data protection practices are in place to safeguard employee privacy. It helps identify and address any potential risks or vulnerabilities related to the collection, storage, and processing of personal data within this environment, thereby ensuring compliance with data protection regulations and preserving the rights and confidentiality of individuals.

The Inteliverse environment, dedicated to operational data, intelligence, and case management, plays a critical role in fraud detection and prevention efforts. As it involves sensitive information related to investigations, intelligence sources, and fraud patterns, a DPIA becomes vital to assess potential risks, evaluate data sharing practices, and implement robust security measures. By conducting a DPIA, the NHSCFA can ensure that adequate safeguards are in place to protect the confidentiality and integrity of the data, maintain compliance, and prevent Unauthorised access or misuse of sensitive information.

Similarly, the HUB environment, with its focus on NHS organisational data and stakeholder engagement, requires a DPIA to identify any privacy risks associated with customer relationship management and data exchange activities. This environment encompasses interactions with external entities, necessitating a careful evaluation of data sharing practices, consent management, and secure communication channels. By conducting a DPIA, the NHSCFA can demonstrate its commitment to protecting stakeholder privacy, maintaining data accuracy, and fostering trust among NHS organisations and key stakeholders.

In summary, the segregation of data models and processes within the Central, Inteliverse, and HUB environments of the Power Platform highlights the need for a DPIA. Conducting a comprehensive DPIA ensures that privacy risks are identified, evaluated, and mitigated effectively. It enables the NHSCFA to implement robust data protection measures, safeguard sensitive information, comply with relevant data protection regulations, and build trust with individuals, NHS organisations, and stakeholders involved in the system/project.

STEP 2: Describe the processing

Describe the nature of the processing:

1. How will you collect, use, store and delete data?
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 are types of processing identified as 'likely high risk' are involved?

1. **Describe the nature of the processing:**
   The processing within the Power Platform involves collecting, using, storing, and deleting data. Data collection occurs through various means such as user inputs, system integrations with NHSCFA applications (e.g., CPOD, LBS), third-party solutions (e.g., iBase, CLUE), and Microsoft services (e.g., Office 365, Teams). The collected data is used for purposes such as workforce management, case management, intelligence analysis, stakeholder engagement, and fraud prevention.

   Data storage is primarily conducted within the Power Platform's environments: Central, Inteliverse, and the HUB. These environments utilise the underlying data storage capabilities of the Power Platform, particularly the Dataverse, to securely store and organise data. Appropriate access controls, encryption, and data retention policies are implemented to ensure data protection.

   Data deletion follows established procedures aligned with data retention policies and legal requirements. When data is no longer needed for its intended purpose or when an individual's consent is withdrawn (if applicable), the data is securely deleted from the relevant systems and environments within the Power Platform.

2. **What is the source of the data?**
   The data collected within the Power Platform originates from multiple sources. These include user inputs provided through Power Apps or other user interfaces, data imported from NHSCFA applications (such as CPOD, LBS, the public website, and the Fraud Manual), data obtained from third-party solutions (e.g., iBase, CLUE, ESR, Go2), and data integrated from Microsoft services (e.g., Office 365, Teams, SharePoint, OneDrive, Outlook).

   The sources of the data may vary depending on the specific environment within the Power Platform. For instance, the Central Environment primarily collects employee-related data, including HR records and employee engagement information. The Inteliverse environment sources operational data, intelligence, and case management data. The HUB environment obtains NHS organisational data and stakeholder engagement information through a CRM built on Power Apps and the Dataverse.

3. **Will you be sharing data with anyone?**
   Data sharing is an integral aspect of the Power Platform's functionality. The platform enables data exchange and collaboration within NHSCFA applications, third-party solutions, and Microsoft services. The sharing of data can occur through various mechanisms, including system integrations, data exports, APIs, and secure communication channels. Sharing of data with external third parties is only applicable to systems that have their own DPIA in place. A copy of which is available on the public website.

   To ensure the security and privacy of PII, the Power Platform implements comprehensive data loss protection policies. These policies are designed to prevent unauthorised sharing, access, accidental data leaks, and intentional or inadvertent data breaches. Data loss protection policies encompass a range of measures, including encryption, access controls, user authentication, and auditing. These measures help safeguard PII and prevent its exposure or misuse.

   Within the Dataverse, access to records is governed by record level access controls. This means

that users are granted permission to view, edit, or delete specific records based on their assigned roles and privileges. Record level access ensures that PII is only accessible to authorised individuals who require access for legitimate business purposes. This granular control helps minimise the risk of unauthorised disclosure or manipulation of PII within the system.

In addition to record level access controls, the Power Platform provides field level access controls. This means that even within a record, specific fields containing sensitive PII can be further restricted in terms of access. Field level access controls allow NHSCFA administrators to define and enforce strict rules regarding who can view or modify specific fields within a record. This adds an additional layer of protection to sensitive PII, ensuring that only authorised individuals with a legitimate need can access or modify such information.

By implementing data loss protection policies, record level access controls, and field level access controls, the Power Platform aims to safeguard PII stored in the Dataverse. These measures mitigate the risk of unauthorised access, data breaches, and misuse of sensitive information. They are instrumental in maintaining compliance with data protection regulations, protecting individual privacy rights, and instilling confidence in the secure handling of PII within the Power Platform.

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

Within the Power Platform, several processing activities can be identified as 'likely high risk':

a. Processing of sensitive personal data: The platform may involve the processing of sensitive personal data, such as employee records, HR data, and potentially confidential fraud-related information. This processing carries a higher risk due to the need for enhanced security measures and strict access controls to protect the privacy and confidentiality of individuals involved.

b. Cross-system data transfers: The integration of NHSCFA applications, third-party solutions, and Microsoft services necessitates data transfers across systems. These transfers involve risks such as data breaches, unauthorised access, or data loss if appropriate security measures are not implemented.

c. Stakeholder engagement and CRM functionality: The HUB environment's processing activities involve stakeholder engagement, communication, and customer relationship management. This includes storing and processing data related to NHS organisations, partners, and other stakeholders. Handling such data requires specific attention to privacy rights, consent management, and secure data handling practices to mitigate potential risks.

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 special category or criminal offence data?
The data processed within the Power Platform includes various types of information relevant to NHSCFA operations. This may include personal data, such as names, contact details, employment information, and case-related details. Additionally, depending on the specific processes and functionalities, the data may involve special category data (sensitive personal data) and, in some cases, criminal offence data. Special category data may include health information, ethnic origin, religious beliefs, or other sensitive information required for fraud prevention and investigation purposes. The processing of special category or criminal offence data requires additional safeguards and compliance with specific legal requirements to ensure the protection of individuals' rights.

2. How much data will you be collecting and using?
The amount of data collected and used within the Power Platform will depend on the specific processes and functionalities employed. This can vary based on the environment within the platform (e.g., Central, Inteliverse, HUB) and the intended purposes. Data may be collected from multiple sources, including NHSCFA applications, third-party solutions, and Microsoft services. The volume of data can range from individual employee records to large datasets related to operational intelligence or stakeholder engagement. Adequate data management practices, including data minimisation and retention policies, are implemented to ensure that only necessary data is collected and used.

3. How often?
The frequency of data collection and processing activities within the Power Platform depends on the operational requirements and workflows. Data may be collected and processed in real-time, such as capturing employee engagement feedback or intelligence updates. Additionally, scheduled data imports, system integrations, or user interactions can occur on a daily, weekly, or monthly basis. The frequency of data processing activities is determined based on the specific needs of the NHSCFA and the relevant applications or processes integrated within the Power Platform.

4. How long will you keep it?
The retention period for data within the Power Platform is determined by legal requirements, operational needs, and data retention policies. The NHSCFA ensures that data is kept only for as long as necessary to fulfill the purposes for which it was collected. Retention periods may vary depending on the type of data and its relevance to ongoing fraud prevention, investigation, or operational activities. Personal data is retained in accordance with data protection regulations, while special category or criminal offence data is subject to additional retention requirements and safeguards

5. How many individuals are affected?
The number of individuals affected by the processing activities within the Power Platform can vary depending on the specific processes and functionalities. It may include NHSCFA employees, stakeholders, NHS organisational representatives, and individuals involved in fraud prevention or investigation activities. The exact number of individuals affected would depend on the scale and scope of the NHSCFA's operations and the specific systems integrated with the Power Platform. The NHSCFA ensures that appropriate privacy measures are in place to protect the rights and confidentiality of all individuals involved.

6. What geographical area does it cover?
The geographical area covered by the Power Platform's processing activities is primarily focused on England and Wales. The system/processes are designed to cater to the requirements of the NHSCFA, which operates within these regions. The data processing activities within the Power Platform are all undertaken within the United Kingdom and comply with the applicable data protection laws and regulations of England and Wales, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.
The geographical scope encompasses NHSCFA operations, NHS organisations, stakeholders, and relevant individuals involved in fraud prevention and investigation efforts within England and Wales.

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)?

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

The nature of the relationship within the Power Platform can be categorised into three main types. Firstly, the NHSCFA as an employer and the individual as an employee. The Power Platform facilitates workforce management, employee engagement, and related activities for NHSCFA employees. This relationship involves the processing of personally identifiable information (PII) relevant to their employment, such as contact details, job roles, and performance data, to effectively manage and engage the workforce.

Secondly, the NHSCFA collaborates with stakeholders from the NHS, wider health groups, government agencies, and other business partners. These stakeholders actively engage with the NHSCFA through the Power Platform for various purposes, including fraud prevention, investigation support, and collaborative initiatives. PII related to these stakeholders, such as contact information, organisational affiliations, and engagement history, may be processed within the Power Platform to facilitate effective communication, collaboration, and stakeholder engagement.

In addition to these relationships, it is important to note that the NHSCFA serves as the national investigative/prevention body for fraud within the NHS. As part of this role, the Power Platform processes PII relating to individuals involved in ongoing and completed fraud investigations and cases. This includes PII such as names, addresses, medical records, financial data, and other relevant information necessary for conducting effective investigations, analysing intelligence, and taking appropriate fraud prevention measures.

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 PII within the Power Platform 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.

2. How much control will they have?

The level of control that individuals have over their data within the Power Platform depends on their specific roles and relationships with the NHSCFA.

For NHSCFA employees, they will have a certain level of control over their personal data. They will be able to access, review, and update some of their own employee information stored within the Power Platform, such as contact details, job activities, and performance data.

For stakeholders from the NHS, wider health group, government agencies, and other business partners, the level of control may vary. They will have the ability to manage their own contact information and communication preferences within the Power Platform. They may also have the option to control their engagement with specific projects, initiatives, or collaborative activities facilitated through the platform.

Regarding individuals involved in ongoing and completed fraud investigations and cases, it is important to note that their level of 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 Power Platform. 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 to inform individuals about their rights, enable them to exercise those rights where applicable, and address any concerns

or queries regarding data processing within the Power Platform.

3. Would they expect you to use their data in this way?
NHSCFA employees would generally expect their data to be used within the Power Platform for workforce management, employee engagement, and related purposes. As employees of the NHSCFA, they understand that their personal data, including contact information, job roles, and performance data, is necessary for the efficient functioning of the organisation and the delivery of their employment-related services. The use of their data within the Power Platform aligns with their expectations as employees of the NHSCFA.

Stakeholders from the NHS, wider health group, government agencies, and other business partners engaging with the NHSCFA through the Power Platform would similarly anticipate that their data will be utilised for collaboration, fraud prevention, investigation support, and stakeholder engagement. These stakeholders actively participate in initiatives facilitated by the NHSCFA and recognise that the processing of their data within the Power Platform is essential for effective collaboration and the achievement of shared goals.

In the case of individuals involved in ongoing and completed fraud investigations and cases, they would reasonably expect their data to be used within the Power Platform for investigative purposes, intelligence analysis, case management, and fraud prevention activities. 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 fulfill the NHSCFA's statutory responsibilities and to support the overall integrity of the investigative process.

The NHSCFA strives to maintain transparency and open communication with individuals regarding the use of their data within the Power Platform. 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.

4. Do they include children or other vulnerable groups?
The processing of data within the Power Platform by the NHSCFA primarily focuses on employees, stakeholders, and individuals involved in fraud investigations and cases within the NHS. While most individuals involved fall into adult categories, it is possible that the data processed within the platform may include information related to children or other vulnerable groups in certain circumstances.

In the case of NHSCFA employees, it is unlikely that children or vulnerable groups would be directly associated with their employment data. The processing of employee data within the Power Platform primarily relates to their roles, responsibilities, and performance within the organisation.

For stakeholders from the NHS, wider health group, government agencies, and other business partners, the data processed within the Power Platform may include information related to children or vulnerable groups in cases where it is directly relevant to the collaborative activities or initiatives being undertaken. However, it is important to note that the NHSCFA takes appropriate measures to handle such sensitive data with utmost care, ensuring compliance with applicable laws and regulations governing the protection of children and vulnerable groups.

Regarding individuals involved in ongoing and completed fraud investigations and cases, it is possible that the data processed within the Power Platform may include information related to children or vulnerable groups. The NHSCFA acknowledges the importance of safeguarding the privacy and welfare of these individuals, especially when dealing with sensitive information. Special considerations and additional measures are in place to protect the rights and interests of children and vulnerable groups involved in the investigative process.

The NHSCFA adheres to applicable data protection laws and guidelines, ensuring that the processing of data within the Power Platform involving children or vulnerable groups is done in a manner that respects their rights, promotes their well-being, and upholds the highest standards of data protection and confidentiality.

5. Are there any prior concerns over this type of processing or security flaws?
The NHSCFA recognises the importance of addressing any prior concerns related to the processing of data within the Power Platform and its various components. To ensure comprehensive data protection, it is important to acknowledge that several specific components within the Power Platform have their own DPIAs in place.

Power BI, as the organisation's data analytics platform, has its own DPIA that covers the processing of data for analytical and reporting purposes. This assessment ensures that the data handled within Power BI is appropriately protected, and any potential risks are identified and mitigated.

Additionally, the NHSCFA has conducted a DPIA for the Central Person Organisation Database (CPOD), which focuses on the processing of stakeholder data. This assessment ensures that the data collected and stored

within CPOD, including information related to stakeholders involved in fraud investigations and cases, is handled securely and in compliance with data protection regulations.

Furthermore, the operational data within the Power Platform, including intelligence and case management data, is covered by the DPIA conducted for the CLUE (NHS National Fraud Case Management System). This assessment ensures that the processing of operational data, such as case information, intelligence reports, and related data, is carried out with appropriate security measures and adherence to privacy principles.

By conducting these DPIAs, the NHSCFA demonstrates its commitment to ensuring data protection and privacy across the Power Platform and its associated components. The NHSCFA actively assesses the potential risks and vulnerabilities associated with each specific area of processing and takes the necessary steps to implement appropriate controls and safeguards.

6. Is it novel in any way?

The use of the Power Platform within the NHSCFA is an innovative approach to enhance operational efficiency, collaboration, and data management. While similar technologies and platforms exist in the market, the specific configurations, integrations, and purposes within the NHSCFA's context may introduce novel aspects. The NHSCFA continuously evaluates emerging technologies and best practices to ensure the Power Platform's alignment with the latest advancements and compliance standards.

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

The Power Platform leverages state-of-the-art technology in data storage, processing, and security. It benefits from the robust infrastructure, data management capabilities, and security measures provided by Microsoft, the provider of the Power Platform. The platform incorporates industry-standard encryption protocols, access controls, authentication mechanisms, and auditing features to ensure the protection of data. Ongoing monitoring and updates to the technology stack are performed to address emerging threats and maintain the highest level of security within the Power Platform.

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

The NHSCFA recognises the importance of public concern regarding data protection, privacy, and the secure handling of personal information. The NHSCFA closely monitors and factors in current issues of public concern related to data processing, security, and privacy. By addressing these concerns, the NHSCFA aims to maintain public trust and confidence in the processing activities carried out within the Power Platform.

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

The NHSCFA holds ISO 27001 certification for information security management and ISO 20000-1 certification for IT service management. These certifications demonstrate the NHSCFA's commitment to maintaining robust security controls and delivering high-quality IT services. The NHSCFA adheres to these internationally recognised standards to ensure the confidentiality, integrity, and availability of data processed within the Power Platform. The certifications provide assurance to individuals and stakeholders that the NHSCFA upholds best practices in managing data security and IT service delivery.

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?
The primary goal of the processing within the Power Platform is to support the NHSCFA in its mission as the national investigative/prevention body for fraud within the NHS. The platform aims to streamline and enhance various aspects of data management, collaboration, intelligence analysis, case management, and stakeholder engagement. By leveraging the Power Platform's capabilities, the NHSCFA seeks to improve operational efficiency, facilitate informed decision-making, enhance fraud prevention and investigation efforts, and ultimately contribute to safeguarding NHS resources.

2. What is the intended effect on individuals?
The intended effect on individuals varies depending on their role and involvement within the NHSCFA and the Power Platform. For NHSCFA employees, the processing within the platform aims to streamline workforce management, improve employee engagement, and support their day-to-day tasks, leading to increased efficiency and job satisfaction.

Stakeholders from the NHS, wider health group, government agencies, and business partners benefit from the Power Platform by enabling seamless collaboration, efficient information sharing, and enhanced stakeholder engagement. This promotes effective fraud prevention, supports investigations, and facilitates the achievement of shared objectives within the healthcare sector.

Individuals involved in ongoing and completed fraud investigations and cases benefit from the processing within the Power Platform through improved case management, intelligence analysis, and fraud prevention measures. 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, for you and more broadly?
The processing within the Power Platform offers numerous benefits for the NHSCFA and the broader healthcare sector. By leveraging the platform's functionalities, the NHSCFA can streamline data management processes, improve collaboration between internal and external stakeholders, enhance operational efficiency, and make well-informed decisions based on comprehensive data insights.

The benefits extend beyond the NHSCFA, as the Power Platform facilitates effective collaboration with stakeholders, promotes information sharing, and supports fraud prevention efforts across the NHS and the wider health group. The platform's capabilities enable more efficient investigation processes, better resource allocation, and enhanced fraud detection, thereby safeguarding NHS resources and ensuring their optimal utilisation for patient care and healthcare services.

Overall, the processing within the Power Platform provides tangible benefits such as improved efficiency, collaboration, informed decision-making, and fraud prevention. These benefits contribute to the NHSCFA's mission of protecting the NHS from fraud and promoting the integrity of the healthcare system, ultimately benefiting the healthcare sector as a whole and the individuals it serves.

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?

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

The NHSCFA will establish channels for consultation and communication, such as surveys, focus groups, or one-on-one discussions, to seek individuals' views on the processing of their data within the Power Platform. However, in certain circumstances where seeking individuals' views may compromise ongoing investigations or pose risks to safety, alternative measures will be implemented to protect confidentiality and privacy.

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

The NHSCFA will involve relevant stakeholders within the organisation, including departments responsible for data governance, legal and compliance, human resources, senior management, and the internal information security (InfoSec) team. The InfoSec team will conduct security reviews independently to ensure compliance with security policies and standards.

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

As the NHSCFA utilises the Power Platform provided by Microsoft, Microsoft acts as a processor for the data processed within the platform. While the NHSCFA does not require direct assistance from Microsoft in conducting the DPIA, the NHSCFA follows the guidance and best practices provided by Microsoft to ensure the secure and compliant utilisation of the platform.

The NHSCFA works closely with Microsoft to understand and implement the recommended security measures, data protection controls, and privacy safeguards within the Power Platform. By aligning with Microsoft's guidelines, the NHSCFA ensures that the processing activities adhere to industry standards and best practices in data protection.

The NHSCFA maintains ongoing communication with Microsoft to stay informed about any updates, enhancements, or security recommendations related to the Power Platform. This collaboration allows the NHSCFA to leverage Microsoft's expertise and ensure that the processing activities within the platform meet the necessary security and privacy requirements.

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

The NHSCFA will primarily rely on its internal InfoSec team for security assessments. However, external information security experts may be engaged if specific expertise or a fresh perspective is needed to enhance the security measures within the Power Platform.

STEP 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

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?

The NHSCFA's lawful basis for processing personal data within the Power Platform is established under the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018. The NHSCFA relies on various lawful bases, including the necessity of processing for the performance of a contract (employment contracts with employees), compliance with a legal obligation (investigation and case management), and legitimate interests pursued by the NHSCFA or a third party (stakeholder engagement and fraud prevention).

2. Does the processing achieve your purpose?

The processing activities within the Power Platform are designed to achieve specific purposes, such as efficient workforce and employee management, effective intelligence, and case management, and streamlined stakeholder engagement. These purposes align with the NHSCFA's mandate as the national investigative/prevention body for fraud within the NHS. The processing enables the NHSCFA to carry out its investigative and preventive functions effectively, enhance operational efficiency, and support decision-making processes.

3. Is there another way to achieve the same outcome?

The NHSCFA continuously assesses and evaluates alternative methods to achieve the desired outcomes. When considering data processing activities within the Power Platform, the NHSCFA examines the feasibility of alternative solutions and technologies. This includes assessing the availability of other secure and compliant platforms or systems that can deliver similar functionalities while maintaining data protection and privacy requirements.

4. How will you prevent function creep?

To prevent function creep within the Power Platform, the NHSCFA has established a comprehensive roadmap and defined milestones to ensure that data processing activities remain aligned with the intended purposes. This includes conducting regular assessments of the platform's functionality, data flows, and user permissions to identify and address any instances of unauthorised access or unintended expansion of data processing activities.

The NHSCFA implements strict access controls and follows the principle of data minimisation, ensuring that individuals are granted access only to the data necessary for their specific roles and responsibilities. User permissions are regularly reviewed and updated based on job functions and changes in organisational requirements. Ongoing monitoring and auditing processes are in place to detect and address any potential function creep issues.

Additionally, the NHSCFA maintains a proactive approach in reviewing and updating its roadmap and milestones to align with evolving business needs, technological advancements, and changes in data protection regulations. This ensures that the processing activities within the Power Platform are

continuously evaluated, and any potential risks of function creep are mitigated.

By following the established milestones and comprehensive roadmap, the NHSCFA maintains control over the scope of data processing within the Power Platform, reduces the risk of unauthorised access or misuse, and ensures that the processing activities remain focused on achieving the intended purposes while safeguarding the privacy and rights of individuals.

5. How will you ensure data quality and data minimisation?

The NHSCFA has established data quality controls and processes within the Power Platform to ensure the accuracy, integrity, and relevance of the data. Data validation rules, data entry guidelines, and regular data cleansing activities are implemented to maintain data quality. Additionally, data minimisation principles are followed, ensuring that only the necessary and relevant data is collected and processed within the Power Platform, reducing the risk of unnecessary data exposure.

6. What information will you give individuals?

Within the NHSCFA's three environments in the Power Platform (Central, Inteliverse, and HUB), individuals will be provided with comprehensive information regarding the processing of their personal data, subject to applicable legal and regulatory requirements. The NHSCFA recognises the sensitivity of certain data related to fraud investigations and cases, and as such, it is important to note that specific information relating to ongoing fraud investigations may not be disclosed to individuals to safeguard the integrity of those investigations.

However, for other areas where personal data is collected, processed, and shared within the Power Platform, the NHSCFA is committed to transparency. Individuals will be informed about the types of personal data that may be collected, such as contact details, employment information, stakeholder affiliations, and relevant professional qualifications. They will be provided with details on the purposes of processing, which may include workforce management, operational intelligence, case management, stakeholder engagement, and collaboration.

The NHSCFA recognises the importance of informing individuals about their rights and how they can exercise those rights. Information regarding individual rights, including access, rectification, restriction, and objection to processing, will be provided. Additionally, individuals will be informed about data retention periods and the mechanisms in place to safeguard their personal data.

To ensure accessibility to information, the NHSCFA's public website will contain comprehensive details about the data collected, processed, and shared within the Power Platform. This includes information about the specific types of data involved, the purposes for processing, and any relevant data sharing arrangements. Individuals can refer to Privacy Policy | NHS Counter Fraud Authority | NHSCFA to find more information about the data practices and their rights.

7. How will you help to support their rights?

The NHSCFA is committed to supporting and upholding the rights of individuals with regards to their personal data within the Power Platform. To ensure that individuals can easily exercise their rights, the following measures will be implemented:

a. Access to Personal Data: Individuals will have the right to access their personal data held within the Power Platform. To facilitate this, the NHSCFA will provide a data access request form on its public website. This form will enable individuals to submit their requests securely and efficiently. The NHSCFA will promptly review and respond to these requests in accordance with applicable data protection laws and regulations.

b. Rectification and Erasure: If individuals find that their personal data within the Power

Platform is inaccurate, incomplete, or no longer relevant for the intended purposes, they have the right to request rectification or erasure. The NHSCFA will establish a dedicated process for handling such requests, ensuring that necessary corrections or deletions are made in a timely manner.

c. Data Portability: Should individuals wish to transfer their personal data to another organisation, the NHSCFA will facilitate data portability as required by applicable data protection laws. The NHSCFA will provide mechanisms to securely transfer the requested data to the designated recipient, ensuring compatibility and compliance with relevant standards.

d. Objection and Restriction: Individuals have the right to object to the processing of their personal data or request restriction of certain processing activities. The NHSCFA will establish clear procedures for individuals to exercise these rights and will carefully evaluate and respond to objections and requests for restriction in the appropriate manner.

e. Privacy by Design: The NHSCFA follows privacy by design principles in the development and operation of the Power Platform. Privacy considerations are incorporated into every stage of the processing activities, ensuring that data protection measures are embedded from the outset.

f. Training and Awareness: The NHSCFA provides regular training and awareness programs to its employees and stakeholders involved in the processing activities. This ensures that they are well-informed about data protection laws, best practices, and their responsibilities in safeguarding individuals' rights.

By implementing these measures, including providing a data access request form on the public website, the NHSCFA aims to empower individuals to exercise their rights effectively and effortlessly. These efforts highlight the NHSCFA's commitment to data protection, privacy, and promoting transparency in the processing of personal data within the Power Platform.

8. What measures do you take to ensure processors comply?

To ensure compliance with data protection regulations, including the General Data Protection Regulation (GDPR), the NHSCFA takes various measures to ensure that processors involved in the processing of personal data within the Power Platform adhere to the necessary standards. These measures include:

a) Due Diligence: The NHSCFA conducts thorough due diligence when selecting processors to ensure they have robust data protection measures in place. This includes assessing their compliance with relevant regulations, their security practices, and their commitment to protecting personal data.

b) Data Processing Agreements: The NHSCFA establishes comprehensive data processing agreements with its processors. These agreements outline the specific obligations and responsibilities of the processors in handling personal data, including requirements for confidentiality, security, and compliance with applicable laws.

c) Regular Audits and Reviews: The NHSCFA performs regular audits and reviews of its processors to ensure ongoing compliance with data protection requirements. This may include conducting security assessments, reviewing data protection policies and procedures, and evaluating the effectiveness of technical and organisational measures implemented by the processors.

d) Documentation and Record-Keeping: The NHSCFA maintains proper documentation and records of its relationships with processors. This includes keeping records of data processing agreements, audit

reports, and any other relevant documentation to demonstrate compliance with data protection regulations.

e) Collaboration with Microsoft: As Microsoft is a processor involved in the Power Platform, the NHSCFA benefits from Microsoft's commitment to data protection and compliance. Microsoft has implemented robust security and privacy measures across its services, including the Power Platform, and provides tools and resources to assist organisations in meeting their compliance obligations. The NHSCFA leverages these resources and collaborates with Microsoft to ensure adherence to regulatory requirements.

By implementing these measures, the NHSCFA strives to ensure that its processors comply with data protection regulations, including the GDPR. The NHSCFA's commitment to working with trusted and compliant processors, combined with regular audits and reviews, enables ongoing monitoring and verification of compliance. This approach helps to safeguard personal data and maintain a high level of data protection within the Power Platform. For more information on Microsoft's compliance with the GDPR, please refer to the following link: Microsoft GDPR Compliance.

9. How do you safeguard any international transfers?

The NHSCFA ensures that all data processed within the Power Platform remains within the UK region. The NHSCFA's Azure tenant is located within the UK, and no data is transferred or processed outside of this region. This approach is in line with the NHSCFA's commitment to data protection and compliance with applicable regulations.

By utilising the UK region of the Power Platform, the NHSCFA benefits from Microsoft's data storage capabilities and security measures specifically designed for the UK region.

Additionally, the NHSCFA follows Microsoft's guidelines and recommendations regarding data storage and security within the Power Platform. Microsoft provides detailed information on how data is stored, secured, and managed within its services, including the Power Platform. This includes adherence to regional data residency requirements and compliance with applicable data protection laws.

The NHSCFA's decision to process all data within the UK region of the Power Platform ensures that personal data remains within the jurisdiction and regulatory framework of the UK. This approach helps to safeguard the privacy and security of individuals' data and aligns with the NHSCFA's commitment to data protection and compliance.

For more information on data storage within the Power Platform and Microsoft's security measures, please refer to the following link: Microsoft Power Platform & Dataverse Data Storage.

STEP 5: Identify and assess risks

ID	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
5.1	**Unauthorised Access:** • Source of Risk: External malicious actors, internal breaches. • Nature of Impact: Privacy breaches, data manipulation, identity theft. • Compliance/Corporate Risks: Non-compliance with data protection regulations, reputational damage.	Possible	Significant	Medium
5.2	**Data Leakage:** • Source of Risk: Inadequate security controls, human error. • Nature of Impact: Exposure of sensitive information, reputational damage. • Compliance/Corporate Risks: Non-compliance with data protection regulations, loss of stakeholder trust.	Possible	Significant	Medium
5.3	**Data Loss:** • Source of Risk: Technical failures, system errors. • Nature of Impact: Permanent loss of critical data, disruption of operations. • Compliance/Corporate Risks: Non-compliance with data protection regulations, operational inefficiencies.	Remote	Severe	Medium
5.4	**Inadequate Data Protection Measures:** • Source of Risk: Insufficient security controls, outdated software. • Nature of Impact: Unauthorised access, data breaches, compromised privacy. • Compliance/Corporate Risks: Non-compliance with data protection regulations, legal penalties.	Possible	Significant	Medium
5.5	**Integration Risks:** • Source of Risk: Incompatible systems, data inconsistencies. • Nature of Impact: Data inaccuracies, process inefficiencies. • Compliance/Corporate Risks: Non-compliance with data integrity standards, operational disruptions.	Possible	Significant	Medium
5.6	**Data Accuracy and Integrity:** • Source of Risk: Human error, system glitches. • Nature of Impact: Incorrect data analysis, flawed decision-making. • Compliance/Corporate Risks: Non-compliance with data accuracy standards, reputational damage.	Probable	Significant	Medium
5.7	**System Downtime:** • Source of Risk: Infrastructure failures, software bugs. • Nature of Impact: Temporary loss of access, operational delays. • Compliance/Corporate Risks: Breach of	Remote	Significant	Medium

	service level agreements, reputational damage.			
5.8	**User Error or Misuse:** • Source of Risk: Lack of user training, negligent actions. • Nature of Impact: Data corruption, system errors. • Compliance/Corporate Risks: Non-compliance with data protection regulations, compromised system security.	Possible	Minimal	Low
5.9	**Inadequate User Training and Awareness:** • Source of Risk: Lack of training programs, insufficient awareness. • Nature of Impact: Unintentional data breaches, security lapses. • Compliance/Corporate Risks: Non-compliance with data protection regulations, increased vulnerability to cyber threats.	Possible	Minimal	Low
5.10	**Regulatory Compliance:** • Source of Risk: Non-compliant data processing practices, evolving regulations. • Nature of Impact: Legal penalties, reputational damage. • Compliance/Corporate Risks: Non-compliance with data protection regulations, loss of stakeholder trust.	Possible	Significant	Medium
5.11	**Insufficient Data Governance:** • Source of Risk: Lack of clear data governance policies and procedures. • Nature of Impact: Inconsistent data management, data integrity issues. • Compliance/Corporate Risks: Non-compliance with data governance regulations, compromised data quality.	Possible	Significant	Medium
5.12	**Inadequate Incident Response:** • Source of Risk: Lack of incident response plans, delayed response times. • Nature of Impact: Prolonged data breaches, increased harm to individuals. • Compliance/Corporate Risks: Non-compliance with incident response requirements, reputational damage.	Possible	Significant	Medium
5.13	**Insecure Third-Party Integrations:** • Source of Risk: Vulnerabilities in third-party applications or APIs. • Nature of Impact: Unauthorised access, data breaches. • Compliance/Corporate Risks: Non-compliance with data protection regulations, legal liabilities.	Possible	Significant	Medium
5.14	**Insider Threats:** • Source of Risk: Malicious actions by employees or contractors. • Nature of Impact: Data theft, Unauthorised access. • Compliance/Corporate Risks: Non-compliance with data protection regulations, reputational damage.	Possible	Significant	Medium

5.15	**Lack of Audit Trails:** • Source of Risk: Inadequate logging and auditing mechanisms. • Nature of Impact: Difficulty in detecting and investigating security incidents. • Compliance/Corporate Risks: Non-compliance with audit trail requirements, hindered incident response.	Possible	Significant	Medium
5.16	**Integration Complexity:** • Source of Risk: Complexity of integrating different systems and data sources. • Nature of Impact: Integration failures, data inconsistencies. • Compliance/Corporate Risks: Non-compliance with data integrity standards, operational disruptions.	Possible	Significant	Medium
5.17	**Lack of Scalability:** • Source of Risk: Inability to handle increasing data volumes and user demands. • Nature of Impact: System performance degradation, operational inefficiencies. • Compliance/Corporate Risks: Non-compliance with service level agreements, hindered business growth.	Remote	Significant	Medium
5.18	**Data Ownership and Retention:** • Source of Risk: Unclear data ownership, retention policy violations. • Nature of Impact: Unauthorised data usage, legal liabilities. • Compliance/Corporate Risks: Non-compliance with data protection regulations, reputational damage.	Possible	Significant	Medium
5.19	**Compliance with Data Subject Rights:** • Source of Risk: Inadequate processes to handle data subject requests. • Nature of Impact: Failure to comply with data subject rights, legal penalties. • Compliance/Corporate Risks: Non-compliance with data subject rights regulations, reputational damage.	Possible	Significant	Medium
5.20	**Ineffective Change Management:** • Source of Risk: Poorly managed system changes and updates. • Nature of Impact: Disruption of operations, data corruption. • Compliance/Corporate Risks: Non-compliance with change management policies, operational inefficiencies.	Possible	Significant	Medium
5.21	**Data Inconsistencies:** • Source of Risk: Lack of data validation and reconciliation procedures. • Nature of Impact: Inaccurate reporting, flawed decision-making. • Compliance/Corporate Risks: Non-compliance with data integrity standards, hindered business insights.	Possible	Significant	Medium
5.22	**Lack of Disaster Recovery:** • Source of Risk: Inadequate measures to recover from system failures or data loss. • Nature of Impact: Prolonged system downtime, data loss. • Compliance/Corporate Risks: Non-	Remote	Significant	Medium

	compliance with service level agreements, reputational damage.			

STEP 6: Identify measures to reduce risk

Identified risk ID	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 Yes/No
5.1	**Unauthorised Access:** • Implement strong access controls, including multi-factor authentication. • Regularly review and update user access permissions. • Monitor and log access activities for potential security breaches. • Conduct regular security assessments and penetration testing. • Encrypt sensitive data to protect against unauthorised access.	Reduced	Low	Yes Approved by AS 28.7.23
5.2	**Data Leakage:** • Implement data loss prevention measures, including encryption and access controls. • Conduct regular audits and monitoring of data access and transfers. • Train employees on data handling and security best practices. • Implement network segmentation to restrict data access to authorised individuals. • Use secure protocols and mechanisms for data sharing and transmission.	Reduced	Low	Yes Approved by AS 28.7.23
5.3	**Data Loss:** • Implement regular data backup procedures and test data restoration processes. • Store backup copies in secure off-site locations or cloud storage. • Implement data redundancy measures to minimise the risk of data loss. • Monitor and address hardware failures and storage issues promptly. • Implement disaster recovery plans to ensure business continuity.	Reduced	Low	Yes Approved by AS 28.7.23
5.4	**Inadequate Data Protection Measures:** • Conduct regular vulnerability assessments and penetration testing. • Implement encryption mechanisms for data at rest and in transit. • Implement access controls and user permissions to limit data exposure. • Regularly update and patch software systems to address security vulnerabilities. • Monitor and address security incidents promptly.	Reduced	Low	Yes Approved by AS 28.7.23

5.5	**Integration Risks:** • Establish comprehensive integration protocols and standards. • Conduct thorough testing of integration processes. • Implement error handling mechanisms and alerts for integration failures. • Regularly review and update integration processes based on feedback and performance metrics. • Implement secure data transfer mechanisms between integrated systems.	Reduced	Low	Yes Approved by AS 28.7.23
5.6	**Data Accuracy and Integrity:** • Implement data validation mechanisms to ensure data accuracy. • Establish data quality monitoring processes. • Conduct regular data audits and integrity checks. • Implement error detection and correction mechanisms. • Provide user-friendly interfaces and input validation prompts.	Reduced	Low	Yes Approved by AS 28.7.23
5.7	**System Downtime:** • Implement proactive monitoring and alerting systems. • Conduct regular system maintenance and updates. • Implement redundancy and failover mechanisms to minimise downtime. • Establish backup and disaster recovery plans. • Perform regular load testing to ensure system scalability and stability.	Reduced	Low	Yes Approved by AS 28.7.23
5.8	**User Error or Misuse:** • Provide comprehensive user training on system usage and best practices. • Implement user access controls and permissions. • Monitor user activities and provide timely feedback and support. • Implement validation and error prevention mechanisms in user interfaces. • Encourage a culture of accountability and responsible data handling.	Reduced	Low	Yes Approved by AS 28.7.23
5.9	**Inadequate User Training and Awareness:** • Develop and deliver comprehensive training programs on platform usage and data handling. • Provide regular reminders and updates on security best practices. • Establish clear policies and procedures for data protection and privacy. • Foster a culture of security awareness and accountability among users. • Conduct periodic assessments to measure user knowledge and address any gaps.	Reduced	Low	Yes Approved by AS 28.7.23

5.10	**Regulatory Compliance:** • Stay up to date with relevant data protection regulations and requirements. • Implement privacy-by-design principles in system design and development. • Conduct regular compliance assessments and audits. • Establish data protection impact assessment (DPIA) processes. • Maintain documentation and records to demonstrate compliance.	Reduced	Low	Yes Approved by AS 28.7.23
5.11	**Insufficient Data Governance:** • Establish clear data governance policies and procedures. • Implement data classification and access control mechanisms. • Assign data ownership and accountability roles within the organisation. • Regularly review and update data governance frameworks. • Conduct periodic data governance audits and assessments.	Reduced	Low	Yes Approved by AS 28.7.23
5.12	**Inadequate Incident Response:** • Develop and implement an incident response plan. • Establish incident response team roles and responsibilities. • Conduct regular incident response drills and simulations. • Monitor and analyse security incidents to identify trends and patterns. • Continuously improve incident response processes based on lessons learned.	Reduced	Low	Yes Approved by AS 28.7.23
5.13	**Insecure Third-Party Integrations:** • Conduct thorough due diligence on third-party vendors. • Implement contractual agreements that address data protection and security. • Regularly review and monitor third-party vendor performance and security practices. • Establish incident response procedures for third-party breaches. • Limit data access and sharing with third-party vendors to necessary information only.	Reduced	Low	Yes Approved by AS 28.7.23
5.14	**Insider Threats:** • Implement user access controls and least privilege principles. • Conduct background checks and screening for employees with system access. • Monitor user activities and establish auditing mechanisms. • Provide security awareness training to employees. • Encourage anonymous reporting channels for suspicious activities.	Reduced	Low	Yes Approved by AS 28.7.23

5.15	**Lack of Audit Trails:** • Implement comprehensive logging and auditing mechanisms. • Capture and retain audit logs of system activities. • Regularly review and analyse audit logs for security incidents. • Implement automated alerts for suspicious or unauthorised activities. • Store audit logs in secure and tamper-proof storage.	Reduced	Low	Yes Approved by AS 28.7.23
5.16	**Integration Complexity:** • Simplify integration processes and eliminate unnecessary complexities. • Implement clear documentation and guidelines for integrations. • Conduct thorough testing and validation of integration processes. • Regularly review and update integration documentation. • Provide support and resources to address integration challenges.	Reduced	Low	Yes Approved by AS 28.7.23
5.17	**Lack of Scalability:** • Perform regular capacity planning to anticipate scalability needs. • Implement scalable infrastructure and systems. • Monitor system performance and capacity metrics. • Continuously optimise system resources for efficiency. • Implement load balancing mechanisms for high-traffic periods.	Reduced	Low	Yes Approved by AS 28.7.23
5.18	**Data Ownership and Retention:** • Clearly define data ownership and responsibilities. • Establish data retention policies and processes. • Regularly review and update data retention guidelines. • Implement secure data disposal processes for expired or unnecessary data. • Document and communicate data ownership and retention guidelines to users.	Reduced	Low	Yes Approved by AS 28.7.23
5.19	**Compliance with Data Subject Rights:** • Establish processes to handle data subject rights requests. • Train employees on handling data subject rights requests. • Implement mechanisms to verify data subject identities. • Maintain records of data subject rights requests and responses. • Regularly review and update data subject rights procedures.	Reduced	Low	Yes Approved by AS 28.7.23

5.20	**Ineffective Change Management:** • Implement change management processes for system updates and modifications. • Conduct impact assessments for changes that may affect data security. • Test changes in a controlled environment before deployment. • Communicate changes and their impact to relevant stakeholders. • Monitor and review the effectiveness of change management processes.	Reduced	Low	Yes Approved by AS 28.7.23
5.21	**Data Inconsistencies:** • Establish data validation mechanisms and business rules. • Conduct regular data quality checks and audits. • Implement data cleansing and normalisation processes. • Establish clear data entry guidelines and standards. • Provide training and support for data entry personnel.	Reduced	Low	Yes Approved by AS 28.7.23
5.22	**Lack of Disaster Recovery:** • Implement comprehensive disaster recovery plans. • Regularly test and validate disaster recovery processes. • Store backup copies of critical data in secure off-site locations. • Establish communication and coordination protocols during a disaster. • Review and update disaster recovery plans based on lessons learned.	Reduced	Low	Yes Approved by AS 28.7.23

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Approved by AS 28.7.23	Also reviewed via the link in Power platform
Residual risks approved by:		
DPO advice provided		
Summary of DPO advice: Having reviewed the DPIA I am satisfied that a comprehensive assessment of the platform has been carried out. Use of the platform will be controlled and overseen by the IT administrators with staff use and access to platform linked to their user accounts and which will therefore be fully auditable. The applications on Microsoft's Power Platform and the Dataverse are essentially cojoined, with the applications facilitating access to and maintaining separation of the Intelligence, Hub and Central data held within the Dataverse. It is within the applications that the user access and control rights are set alongside parameters for retention, privacy etc. The applications within the platform do not separately hold any personal data within their own right, they only act as a portal to the information held in the Dataverse. 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:	Trevor Duplessis - 28th July 2023	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 DPO should also review ongoing compliance with DPIA

Ownership

16. The following table describes the roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	NHSCFA Corporate Information Asset Owners
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Information Systems and Security
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that Microsoft Power Platform & Dataverse, and any 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.

The Privacy and Electronic Communications Regulations

4. 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

5. 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

6. 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

7. There are no residual privacy risks to the personal data recorded in the platform. 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.

Annex B - Data Protection Compliance Check Sheet

PART 1: BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1. Organisation and project.

Organisation	NHSCFA
Branch / Division	NHSCFA – ISS
Project	Microsoft Power Platform & Dataverse

2. Contact position and/or name
(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

Name, Title	Trevor Duplessis
Branch / Division	Information Governance, NHSCFA

3. Description of the programme / system / technology / legislation (initiative) being assessed. (Please note here if the initiative does not collect, use or disclose personal data*). If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

As detailed above.

4. Purpose / objectives of the initiative (if statutory, provide citation).

As detailed above.

5. What are the potential privacy impacts of this proposal?

As detailed above.

6. Provide details of any previous DPIA or other form of personal data* assessment done on this initiative (in whole or in part).

This is the first DPIA carried out on the platform.

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO PART 3: DPA COMPLIANCE - CONCLUSIONS

*IMPORTANT NOTE: 'Personal data' means data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Page left intentionally blank.