NHS Counter Fraud Authority

Easy Expenses System

Data Protection Impact Assessment

August 2021

V2.1 Published

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

Executive Summary

This document contains information in relation to the Easy Expenses System.

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 (May 2018).

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

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

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

Easy Expenses System General Description 7

Data Protection Impact Assessment 8

Ownership 19

2. DPIA Report: **19**

Section 1: Overview of Data Collection and Maintenance 19

Section 2: Uses of the Application and the Data 20

Section 3: Data Retention 20

Section 4: Internal Sharing and Disclosure of Data 20

Section 5: External Sharing and Disclosure of Data 20

Section 6: Notice/Signage 20

Section 7: Rights of Individuals to Access, Redress and Correct Data 21

Section 8: Technical Access and Security 21

Section 9: Technology 21

3. Compliance Checks **21**

DPA 2018 Compliance Check 21

The Privacy and Electronic Communications Regulations 22

The Human Rights Act 22

The Freedom of Information Act 22

Conclusion 22

Annex A - Definition of Protected Personal Data **23**

Annex B - Data Protection Compliance Check Sheet **24**

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Corporate Governance Manager Board Secretary	DPIA Easy Expenses System	DPO	V0.1 -V0.3	Oct-Dec 2020	Initial creation
Corporate Governance Manager and Board Secretary	DPIA Easy Expenses System	DPO	V0.4	Jan 21	Queries answered by from Giltbryte included
Corporate Governance Manager and Board Secretary	DPIA Easy Expenses System	DPO	V0.5	Jan 21	For TD review pending raising remaining query with SMT concerning ownership
Corporate Governance Manager and Board Secretary	DPIA Easy Expenses System	DPO	V0.6	Jan 21	For approval by TD
Corporate Governance Manager and Board Secretary	DPIA Easy Expenses System	DPO	V1.0	Jan 21	Approved
Corporate Governance Manager and Board Secretary	DPIA Easy Expenses System	DPO	V2.0	Aug 21	Redacted for publication
Corporate Governance Manager and Board Secretary	DPIA Easy Expenses System	DPO	V2.1	Feb 2023	Slight Redaction. Original completion date retained as no change to process

Prefix	
Reference:	**DPIA Easy Expenses**
Date:	**August 2021**
Author:	**Corporate Governance Manager and Board Secretary**
Data Owner & DPIA responsibility :	**FCG & ISA stakeholders**
Version:	**2.1**
Supersedes	**2.0**

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	May 2018	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 effect 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.

Easy Expenses System - General Description

10. The EASY system is a system which will facilitate NHSCFA people to claim expenses. e.g. for travel and subsistence. All NHSCFA will have access to the system to claim expenses, and the number of NHSCFA people able to authorise expenses will be restricted to those with line management authority.

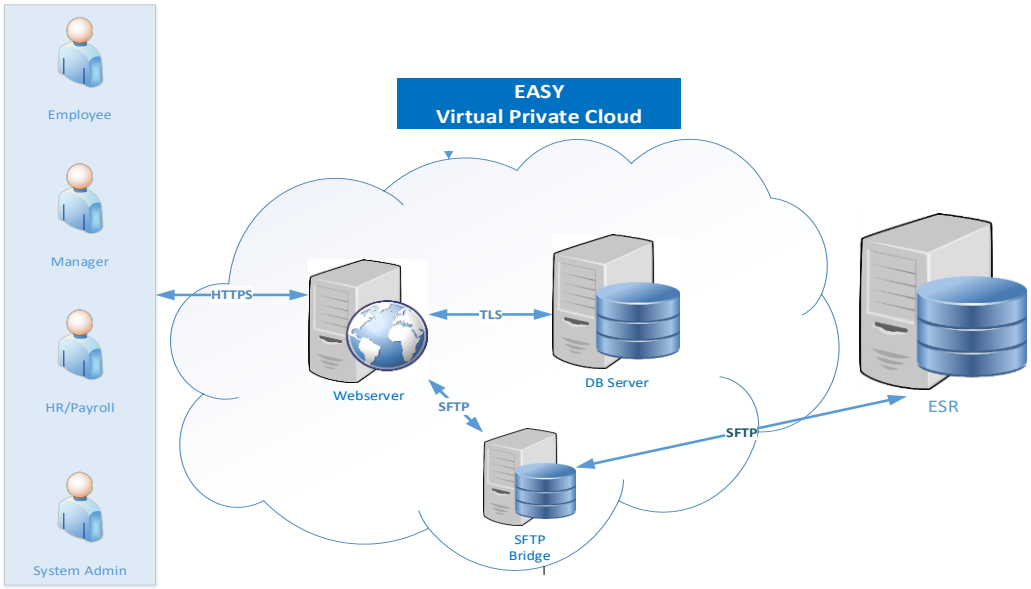
    The EASY software programs are web-based applications accessed by W3C standard compliant web browsers, such as Google Chrome, Mozilla Firefox, Opera, Safari or Internet Explorer version 9 or above.

    The EASY system is underpinned by the cloud computing resources of Amazon Web Services which are UK based operating out of their London Data Centre(AWS). This is based on virtual server architecture, configured and managed by Giltbyte as part of our Hosted Service

11. The following categories of data may be stored in the EASY database: Employee Personal Details, including person identifiable, Employment Details, Vehicle Details, Expense Claim Details

The data will be collected via direct input from the claimant and information is shared between ESR and EASY using the standard outbound and inbound interface files. These are transferred between the two systems using SSH File Transfer Protocol (SFTP) This Protocol provides encryption of the data in transit.

The high-level data flow is shown below



12. This is the first DPIA to be completed on the system. And It has been carried out by the Information and Records Management Officer, in consultation with the Corporate Governance and Board

Secretary (Project Manager), the Information Systems Lead, the Service Support Specialist, and the Director of Finance & Corporate Services and the Information Governance and Risk Management Lead.

13. The Easy Expenses System 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.

Data Protection Impact Assessment

14. To ensure the Easy Expenses System 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 or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The EASY system is a system which will facilitate NHSCFA people to claim expenses. E.g. for Travel and subsistence. All NHSCFA people will have access to the system to claim expenses. The number of NHSCFA people able to authorise expenses will be restricted to those with line management authority. The EASY software programs are web-based applications accessed by W3C standard compliant web browsers, such as Google Chrome, Mozilla Firefox, Opera, Safari or Internet Explorer version 9 or above. The EASY system is underpinned by the cloud computing resources of Amazon Web Services (AWS). This is based on virtual server architecture, configured and managed by Giltbyte as part of our Hosted Service with the BSA. Information is shared between ESR and EASY using the standard outbound and inbound interface files. These are transferred between the two systems using SSH File Transfer Protocol (SFTP) . Data is extracted from Easy with no write back option It is considered a DPIA assessment is required due to the fact data sets will be matched to the payroll system and personal data will be retained.

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?

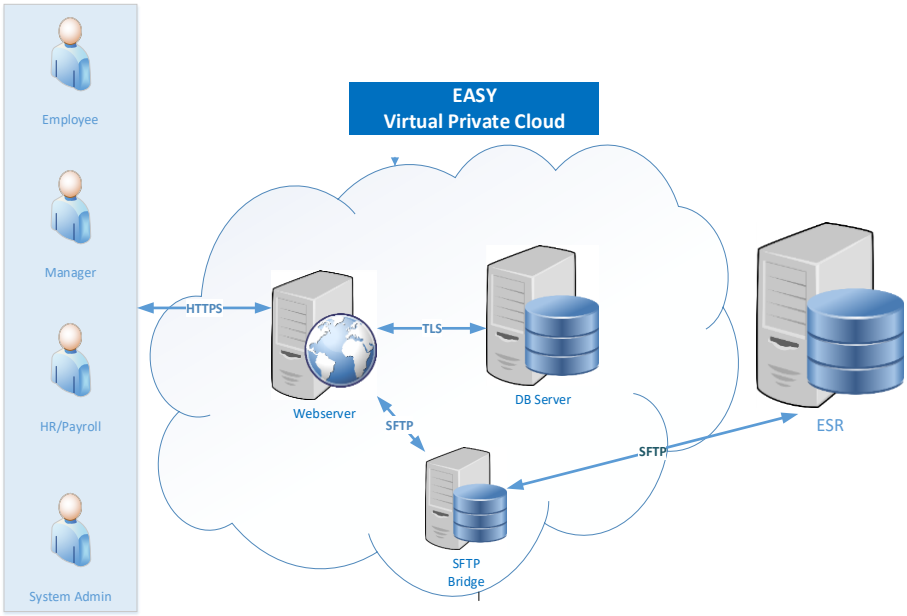
3. Will you be sharing data with anyone (consider using a flow diagram or other way of describing data flow)?

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

1 Data will be collected via interface with ESR and by direct input by claimants (NHSCFA people)

2 Source data will be that within ESR this will include personal and sensitive data e.g. names, addresses line management responsibilities

3 The data will be shared with individual line managers, admin users at Giltbyte to resolve queries and the NHSBSA to facilitate payment



4 The risks associated with data processing has been mitigated against. See step 5 non are rated as high risk.

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. The data includes names, addresses and vehicle details,
   - Name
   - Email address
   - Home address
   - Employee number
   - Dob
   - NI Number
   - Work location & job title
   - Ethnic origin
   - Sickness details (may be included)
   - Hours worked/expenses incurred
   - Automatic collection of details of your internet connection
   - amounts claimed and copies of receipts.

It does not include criminal offence data

2. Data necessary to assess, authorise and pay travel and subsistence expenses will be collected on a regular basis from all NHSCFA people

3. Regularly as NHSCFA people incur expenses whilst on official business.

4.6 years as it is financial information
5. 168 FTE.

6. It will cover England. This applies to all NHSCFA staff both office and home based

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. All NHSCFA employees 2.System access will be restricted by password management depending on access level required 3.Yes, all NHSCFA people expect their expenses to be paid and understand the requirement to hold data for this purpose 4. No 5. No 6. No 7. This is a specific accepted business tool already in use by a variety of organisations. 8. No 9. The NHSCFA has an ISO ISO27001:2013 certification on information security which covers information processed within the NHSCFA network. The certification held for Easy Expenses is explained in Step 4 below.

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. Payment of expenses to NHSCFA People and to provide and auditable system for audit and tax purposes.

2. They receive payment

3. The adoption of EASY system brings the payment of expenses in house,/provide more control of staff information/ ease of process etc.

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. Individual staff consultation was not appropriate, but the necessary Management and PM consultations took place. The consultations took place prior to the PID being approved. Without this system there will be no ongoing ability to make expenses payments.

2. All NHSCFA people in respect of making a clam. ISA as system administrators, FCG for the workflow requirements.

3. No

4. Internal consultation with NHSCFA ISA and external consolation NHS BSA payroll & Finance Teams

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.Contract

2. Yes

3. No

4.The parameters of the system are limited to specific use

5.Individuals are responsible for making sure their data is up to date and correct; only the use of data required for the payment of expenses will be processed. Payment information will not be kept for longer than necessary

6. Guidance documents for use of the system

7. NHSCFA have a range of policies and procedures in place for maintaining compliance with DPA and a range of safeguards for retaining data securely against cyber attacks including ISO27001 accreditation and audit arrangements.

8.Easy Expenses Quality Management System has been certified as meeting the ISO 9001 standard. and the Information Security Management System has attained the ISO 27001 accreditation.

9. In accordance with the Data Protection Act and the NHS Information Governance guidelines, data is not transferred outside of the EU

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
Risk of hosting server failure : In addition to nightly backups, the database servers offer a point in time recovery that means that there is minimal loss of data in the event that data recovery is necessary. As part of our business continuity testing, we have been able to fully restore services to larger organisations within two hours.	Possible	Minimal	Low
Risk of IT failure due to events other events e.g. fire, flooding, force majeure: The use of the AWS facilities ensure that IT failures due to environmental and power outages are extremely low.	Remote	Significant	Low
Risk the interface with payroll fails resulting in CFA people not being paid expenses. The file extraction has been tested and protocols are in place with the BSA who received this to process as part of the BSA MoU requirements.	Remote	Significant	Low
Data held is accessed by Cyber criminals: the required mitigations are in place to ensure data security including virus protection, system monitoring and vulnerability patching.	Remote	Severe	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** Yes/No
All are assessed as low - No additional measures currently identified over and above those in place			

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		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:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments: Having reviewed the DPIA I am satisfied that a comprehensive assessment of the platform has been undertaken. The use and storage of personal data is limited to that only required to achieve the stated purpose with appropriate information provided/made available to data subjects. There is no direct interconnectivity with other data systems, with use of the platform controlled and overseen by the IT administrators and limited permission-based access 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 organisational security measures employed.		
Consultation responses reviewed by:	Trevor Duplessis - 11th January 2021	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

The following table describes the roles and responsibilities

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owners (IAO)	FCG/ISA LT leads
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	NHSCFA do not own or manage the database this is covered by Giltbryte's DPIA
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

1. DPIA Report:

Section 1: Overview of Data Collection and Maintenance

1. The EASY system is a system which will facilitate NHSCFA people to claim expenses. e.g. for Travel and subsistence.

2. The following categories of data may be stored in the EASY database: Employee Personal Details, including person identifiable, Employment Details, Vehicle Details, and Expense Claim Details

3. The impact level of the Easy Expenses System was assessed as OFFICIAL and it can only be accessed internally.

4. The following measures briefly describe what controls have been implemented to protect the system and the personal data recorded:

    a. All NHSCFA will have access to the system to claim expenses. The number of NHSCFA people able to authorise expenses will be restricted to those with line management authority.

    b. The system does not have any direct interconnections with other NHSCFA systems and applications. The data will be collected via direct input from the claimant and via interface with ESR to repopulate information e.g. authorisation access

    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.

5. It is assessed that there are no residual privacy risks to the personal data used by the system.

6. 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

7. The adoption of EASY system brings the payment of expenses in house,/provide more control of staff information/ ease of process etc.

8. NHSCFA responsibility is restricted to user access authorisations and raising support calls.

9. Information in the system could include Employee Personal Details, including person identifiable, Employment Details, Vehicle Details and Expense Claim Details.

10. Sensitive data included Personal identifiable information e.g. names, address, bank account,

11. 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

12. The Easy Expenses System is subject to NHSCFA Data Handling and Storage Policy. Records are marked for deletion as the end of the data retention period.

13. 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

14. All NHSCFA will have access to the system to claim expenses. The number of NHSCFA people able to authorise expenses will be restricted to those with line management authority.

Section 5: External Sharing and Disclosure of Data

15. The only information shared with external organisations, would be if it was requested for the administration of justice and [if shared with other organisations need to state/confirm this is being done in accordance with appropriate Information Sharing Agreement/Memorandum of Understanding

Section 6: Notice/Signage

16. 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.

17. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to this Database/System and therefore outside the scope of this DPIA.

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

18. 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.

19. It is unlikely that any access requests will be received Individuals are responsible inputting their own data and are aware of what is retained in the system.

20. In the unlikely event that information is identified as being incorrect, NHSCFA staff will take appropriate steps to correct the record where permissible or raise a support call via the helpdesk.

21. 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

22. The security and technical access architecture of the Database/System is as explained in this DPIA:

The application and the hosting infrastructure was assessed at **Official**

23. Access is restricted to internal staff only.

24. The technical controls to protect the database include: virus protection, system monitoring and vulnerability patching. Access to the servers is permission based and fully logged.

Section 9: Technology

25. The Database/System holds personal information inputted manually by individuals and is retained on the data server as detailed earlier.

2. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the system, 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.

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 System. 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 FCG & ISA
Project	Easy Expenses System

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	Finance and Corporate 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.

The EASY system is a system which will facilitate NHSCFA people to claim expenses. E.g. for Travel and subsistence.

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

The introduction of this system will bring the payment of expenses in house, to provide more control of staff information and also ease of process. All NHSCFA people will have access to the system in order to claim expenses. However the number of NHSCFA people able to authorise expenses will be restricted to those with line management authority.

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

Data Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data in the Easy Expenses System has been gathered for a specific, justifiable and proportional purpose and found to be mitigated by the steps put in place to minimise the possibility of unauthorised access or use (see Compliance Checks in section 3 of this document)

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 system.

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.

NHSCFA offices

Coventry

Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

4th Floor
Skipton House
80 London Road
London
SE1 6LH

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH