**Data Protection Impact Assessment**

# Introduction

The Data Protection Impact Assessment (DPIA) process is an important means of evidencing our compliance with the requirements of the Data Protection Act 1998 and, from May 25th 2018, the General Data Protection Regulations 2016.

|  |  |
| --- | --- |
| The DPIA should be completed with the help of the accompanying guidance. |  |

Where we are introducing new (or amending existing) systems or processes which involve personal data, the proposal will be reviewed against a set of criteria which determines whether it needs to be formally assessed under a DPIA.

The DPIA process will capture:

* *Requirements:* Any compliance issues with the initial requirements of a proposed change
* *Design:* Approval of a design which brings any compliance issues within our risk tolerance
* *Build & Test:* Final confirmation that the implemented change satisfies the agreed measures identified during the process

Completed DPIAs will form part of our ‘Record of Processing Activity’ which documents our practice and provides assurance that we comply with our statutory data protection responsibilities.

This DPIA should be completed by the Project/initiative Manager, with the help of assigned DPO. The associated guidance document should be consulted for help in defining terms and processes.

# The Proposal

|  |  |  |
| --- | --- | --- |
|  | **About this Assessment** |  |
|  |  |  |
|  | Title of Project: |  |  |
|  | **Brief summary and description of the project:** |  |
|  |  |  |
|  |  |  |  |

**Contact details for initiative**

|  |
| --- |
| **Person completing this assessment (Author) e.g. Project Manager, Information Asset Manager** |
| **Name** |  |
| **Job Title** |  |
| **Department** |  |
| **Contact address**  |  |
| **Email address** |  |
| **Telephone number** |  |
| **Connection to initiative**  |  |

|  |
| --- |
| **Initiative lead e.g. Project Director, Information Asset Owner (IAO)** |
| **Name** |  |
| **Job Title** |  |
| **Department** |  |
| **Contact address**  |  |
| **Email address**  |  |
| **Telephone number** |  |
| **Connection to initiative e.g. IAO**  |  |

# DPIA Risk Assessment

**Assessment of the proposal against the GDPR ‘High Risk’ criteria requiring a DPIA**

|  |  |  |
| --- | --- | --- |
|  | **High Risk Processing**  |  |
|  |  |  |
|  | Does the processing meet the criteria of ‘high risk’ processing? | Yes[ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

# The Data

|  |  |  |
| --- | --- | --- |
|  | **Personal data processed** |  |
|  | Please indicate which of the following personal data will be used |  |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| Forename |[ ]  Surname |[ ]  Postal address |[ ]  Post Code |[ ]
| Email address |[ ]  Age |[ ]  Date of Birth |[ ]  Gender |[ ]
| NI Number |[ ]  NHS Number |[ ]  Image (i.e. photo/video of person) |[ ]  Online identifier |[ ]
| Other unique ID numbers or codes (please specify): |
| Other identifiers (please specify): |

 |  |
|  |  |  |  |

|  |  |
| --- | --- |
| **‘Special Categories’ of Personal Data (sensitive personal data)** |  |
| Tick a box if the Personal Data processed fits into a relevant ‘Special Category’ below.  |  |
|  | Religion or philosophical beliefs |[ ]  Biometric or Genetic data  |[ ]   |
|  | Race or ethnic origin |[ ]  Health  |[ ]   |
|  | Political opinions |[ ]  Sex life or sexual orientation |[ ]   |
|  | Trade-union membership |[ ]  Criminal convictions  |[ ]   |
|  |  |

|  |  |
| --- | --- |
| **Categories of Data Subject** |  |
| Tick a box next to the categories of data subject whose personal data will be processed  |  |
|  | Customers |[ ]  Complainants (& Reps)  |[ ]  Employees/ Contractors |[ ]   |
|  | Suppliers |[ ]  Advisors/ Consultants |[ ]  Captured on CCTV |[ ]   |
|  | Carers (& Reps) |[ ]  Incident witnesses |[ ]  Employees of other Orgs |[ ]   |
| Other (please specify) |  |

|  |  |
| --- | --- |
| **Data format** |  |
| Please indicate which of the following formats are used for the data  |  |
|  | Audio tape/cassette |[ ]  Digital document  |[ ]  Digital image |[ ]   |
|  | Digital video |[ ]  Email |[ ]  Microfilm |[ ]   |
|  | Paper documents |[ ]  Video tape/cassette |[ ]  Web content |[ ]   |
| Other (please specify):  |  |

|  |  |  |
| --- | --- | --- |
|  | **Incoming data flows (data sent from third party to Treetops)** |  |
|  |

|  |  |
| --- | --- |
| Tick box if there are **no** incoming data flows | [ ]  |
| Name of Provider | Data format | Method of sending | Received by |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Add rows as necessary |  |  |

|  |  |  |
| --- | --- | --- |
|  | **Internal data flows (data shared with other teams or systems within Treetops)** |  |
|  |

|  |  |
| --- | --- |
| Tick box if there are **no** internal data flows | [ ]  |
| Name of team sending | Data format | Method of sharing | Received by |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Add rows as necessary |  |  |
|  | **Outgoing data flows (data sent by Treetops to third parties)** |  |
|  |

|  |  |
| --- | --- |
| Tick box if there are **no** outgoing data flows | [ ]  |
| Name of Recipient | Data format | Method of sending | Sent by |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Add rows as necessary |  |  |

# The Principles

## Processed lawfully, fairly and in a transparent manner

### Legal basis for processing

|  |  |  |
| --- | --- | --- |
|  | **Conditions for Processing**  |  |
|  | Tick all relevant conditions which apply to the processing of personal and special category data.To ensure the processing can be done lawfully at least one of the conditions must apply in the first column in relation all personal data and, if processing special categories of personal data, at least one in the second column. |  |
|  |  |  |
|  | 1. **Personal Data**
 | 1. **Special Categories**
 |  |
|  | 6(1)(a) | Consent  |[ ]  9(2)(a) | Explicit Consent  |[ ]   |
|  | 6(1)(b) | Contracts to which the data subject is a party |[ ]  9(2)(b) | Employment, Social Security, Social Protection law |[ ]   |
|  | 6(1)(c) | Legal obligation |[ ]  9(2)(c) | Vital interests  |[ ]   |
|  | 6(1)(d) | Vital interests |[ ]  9(2)(d) | Not-for-profit body |[ ]   |
|  | 6(1)(e) | Task carried out in the Public Interest or under Official Authority. |[ ]  9(2)(e) | Made public by the data subject |[ ]   |
|  | 6(1)(f) | processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. |[ ]  9(2)(f) | Legal claims / Judicial  |[ ]   |
|  |  | 9(2)(g) | Substantial Public Interest |[ ]   |
|  |  | 9(2)(h) | Medicine, Employee capacity, Medical Diagnosis, Health or Social Care |[ ]   |
|  |  | 9(2)(i) | Public Health |[ ]   |
|  |  | 9(2)(j) | Archiving, Scientific and Historical Research or Statistical Purposes in the public interest |[ ]   |
|  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **Legal Gateway** |  |
|  |  |  |
|  | List any applicable legislation that applies to the processing |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | (add additional entries as required) |  |

|  |  |  |
| --- | --- | --- |
|  | **Consent**  |  |
|  |  |  |
|  | If consent is being relied upon, confirm that the relevant conditions are in place |[ ]   |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

### Rights (*please refer to the guidance document for help with this section*)

|  |  |  |
| --- | --- | --- |
|  | **The Right to be Informed** |  |
|  |  |  |
|  | Does the processing support this right? | Yes [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **The Right of Access** |  |
|  |  |  |
|  | Does the processing support this right? | Yes [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **The Right to Rectification** |  |
|  |  |  |
|  | Does the processing support this right? | Yes [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **The Right to Erasure** |  |
|  |  |  |
|  | Does the processing support this right? | Yes [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **The Right to restrict Processing** |  |
|  |  |  |
|  | Does the processing support this right? | Yes [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **The Right to Data Portability (only applicable if reliance on consent)** |  |
|  |  |  |
|  | Does the processing support this right? | Yes [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **The Right to Object** |  |
|  |  |  |
|  | Does the processing support this right? | Yes [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **Rights related to automated decision making and profiling** |  |
|  |  |  |
|  | Does the processing support this right? | Yes [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

### Data Subject consultation

|  |  |  |
| --- | --- | --- |
|  | **Describe any consultation with Data Subjects over appropriate processing of personal data** |  |
|  |  |  |
|  | Has any consultation been undertaken with Data Subjects? | Yes [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

## Collected for specified, explicit and legitimate purposes

|  |  |  |
| --- | --- | --- |
|  | State the ‘purpose(s)’ for which personal data is being obtained |  |
|  |  |  |  |
|  | Purpose 1 |  |  |
|  | Purpose 2 |  |  |
|  | Purpose 3 |  |  |
|  | (add additional entries as required) |  |

|  |  |  |
| --- | --- | --- |
|  | Further processing |  |
|  |  |  |
|  | Confirm that no further use is intended to be made of the data |[ ]   |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

## Adequate, Relevant and Limited

|  |  |  |
| --- | --- | --- |
|  | **Minimising Personal Data** |  |
|  |

|  |  |  |
| --- | --- | --- |
| Are the personal data being obtained a minimal amount necessary to fulfil the purposes above (if not please explain reasons why not below) | Yes | No |
|  |[ ] [ ]

 |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **Pseudonymisation or anonymisation** |  |
|  |

|  |  |  |
| --- | --- | --- |
| Will pseudonymisation or anonymisation processes take place (*if so, please describe below*) | Yes | No |
|  |[ ] [ ]

 |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

## Accurate and, where necessary, kept up to date

|  |  |  |
| --- | --- | --- |
|  | **Accuracy** |  |
|  |  |  |
|  | Confirm that there is a process in place for ensuring that personal data is accurate and is reviewed where necessary |[ ]   |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

## Kept no longer than is necessary

|  |  |  |
| --- | --- | --- |
|  | **Retention** |  |
|  |  |  |
|  | The process effectively manages retention of personal data and is aligned to the Organisation’s published retention schedule |[ ]   |
|  | List the relevant Retention Period(s): |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

## Appropriate Security

### Organisational Controls

1. ***Procurement***
2. (If your project does not involve a tender process or require a contract please leave blank and move on to c) training)

|  |  |  |
| --- | --- | --- |
|  | **The Tender process:** |  |
|  | Based on the risk rating of the data, this is the level of assurance required for the procurement process |  |
|  |  |  |  |
|  | Procurement Assurance requirement | Select |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Contractual Control:** |  |  |
|  |  |  |  |
|  | The contract contains the Organisation’s standard contract schedule relating to Information Governance requirements | [ ]  |  |
|  | If the schedule is not in the contract, what equivalent control is in place? |  |
|  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **Contract Term:** |  |
|  |  |  |  |  |  |
|  | Start Date: |  | End Date: |  |  |
|  | Optional extension period (years): |  |  |
|  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **The Selected Supplier(s)** |  |
|  | Supplier Name(s)  |  |
|  | Supplier Name | Accredited |  |
|  |  | [ ]  |  |
|  |  | [ ]  |  |
|  |  | [ ]  |  |
|  |  | [ ]  |  |
|  | (add additional entries as required for framework contracts/ ‘lot’ winners) |  |

1. ***Training***

|  |  |  |
| --- | --- | --- |
|  | **Training in how to securely process the data** |  |
|  |  |  |
|  | Confirm that employees (and users where relevant) of the system will receive appropriate training |[ ]   |
|  | Confirm that comprehensive written guidance will be available to employees and users  |[ ]   |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

1. ***Policy***

|  |  |  |
| --- | --- | --- |
|  | **Capture issues impacting on Organisational Policy** |  |
|  |  |  |
|  | Confirm that the proposal does not impact current Organisational Policy in a way that requires a review of a Policy’s adequacy? (identify affected Policies below) |[ ]   |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

### Technical Controls

1. ***Access***

|  |  |  |
| --- | --- | --- |
|  | **Access controls**  |  |
|  |  |  |
|  | Confirm that the Access Controls in place will effectively ensure that only those with a valid need to access the data can do so | [ ]  |  |
|  | Confirm that the Access Controls in place will effectively ensure that a management scheme is in place which assigns and reviews appropriate permissions to view, create, amend and delete data | [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

1. ***Security at Rest***

|  |  |  |
| --- | --- | --- |
|  | **Securing the data within a system**  |  |
|  |  |  |
|  | Confirm that appropriate technical security is in place to protect the data at rest from threats appropriate to the security classification of the data | [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

1. ***Security in Transit***

|  |  |  |
| --- | --- | --- |
|  | **Securing the data when transferred from one system to another**  |  |
|  |  |  |
|  | Confirm that appropriate technical security is in place to protect the data in transit from threats appropriate to the security classification of the data | [ ]  |  |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

# Transfer outside the EEA

|  |  |  |
| --- | --- | --- |
|  | **Transfer of Personal Data to countries outside the EEA** |  |
|  |  |  |
|  | No personal data is anticipated being transferred to outside of the EEA, but the project manager will refer to the Data Protection Officer for assessment if a need arises  |[ ]   |
|  | There is an expectation that it may be necessary to transfer personal data to countries outside of the EEA and this activity will meet the required criteria in law (please identify the countries below) |[ ]   |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

# Risk Management

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Risk Description** | **Mitigating Control(s)** | **Likely** | **Impact** | **Score** |
| **1** |  |  | Select | Select | Select |
| **2** |  |  | Select | Select | Select |
| **3** |  |  | Select | Select | Select |
| **4** |  |  | Select | Select | Select |
| **5** |  |  | Select | Select | Select |
| **6** |  |  | Select | Select | Select |
| **7** |  |  | Select | Select | Select |

(Add rows as necessary)

  

# Attachments

Please embed relevant documents below.

This section and the documents within will not be routinely published with the DPIA.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | **Document** | **Title/ Summary** |  |
|  |  |  |
|  | **Information Governance/Legal** (Privacy Notice/ Consent Form) |  |
|  | [Embed Doc] |  |  |
|  | [Embed Doc] |  |  |
|  | **Project** (including Business Case, PIDs, training docs; procedures, etc.) |  |
|  | [Embed Doc] |  |  |
|  | [Embed Doc] |  |  |
|  | [Embed Doc] |  |  |
|  | **Design** **& ICT Security** (including Spec; security assessments, network diagrams etc.) |  |
|  | [Embed Doc] |  |  |
|  | [Embed Doc] |  |  |
|  | [Embed Doc]  |  |  |
|  | **Procurement** (including IG evaluation(s), Contract/ Agreement)  |  |
|  | [Embed Doc] |  |  |
|  | [Embed Doc] |  |  |
|  | [Embed Doc] |  |  |
|  |  |  |  |

# Reviews

|  |  |  |
| --- | --- | --- |
|  | **Regularity of Reviews** |  |
|  |  |  |
|  | The processing does not meet the criteria requiring a review |[ ]   |
|  | A timetable for reviewing the processing has been identified, taking into account the intended length of the activity and the risk rating  |[ ]   |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

**Review Outcomes**

|  |  |  |
| --- | --- | --- |
|  | **Review 1** |  |
|  | Where items below cannot be ticked, explain why in the comments and explain what action is to be taken |  |
|  | Date Review Undertaken:  |  |  |
|  | Confirm that the processing as initially approved in this assessment remains unchanged |[ ]   |
|  | All mitigations remain in place and are effective and appropriate to the level of risk  |[ ]   |
|  | No further action is required as a result of the review |[ ]   |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **Review 2** |  |
|  | Where items below cannot be ticked, explain why in the comments and explain what action is to be taken |  |
|  | Date Review Undertaken:  |  |  |
|  | Confirm that the processing as initially approved in this assessment remains unchanged |[ ]   |
|  | All mitigations remain in place and are effective and appropriate to the level of risk  |[ ]   |
|  | No further action is required as a result of the review |[ ]   |
|  | ***Comments:*** |  |
|  |  |  |
|  |  |  |  |

 (Add additional sections for further reviews)

# Approvals

|  |
| --- |
| **Stage 1 – Requirements Approval (IGIA Stage)** |
| *Function/Role* | *Officer Approving (Name)* | *Date* | *Comments* |
| Role 1 |  |  |  |
| Role 2 |  |  |  |
|  |
| **Stage 2 – Design Approval (LLD Stage)** |
| *Function/Role* | *Officer Approving (Name)* | *Date* | *Comments* |
| Role 1 |  |  |  |
| Role 2 |  |  |  |
|  |
| **DPO Sign-off (Design approval – if required)** |
| *Function* | *Officer Approving (Name)* | *Date* | *Comments* |
| DPO |  |  |  |
|  |
| **Stage 3 – Build & Test Approval (All IG mitigations have been delivered in the live solution)** |
| *Function/Role* | *Officer Approving (Name)* | *Date* | *Comments* |
| Role 1 |  |  |  |
| Role 2 |  |  |  |
|  |
| **DPO Sign-off (Build & Test Approval – if required)** |
| *Function* | *Officer Approving (Name)* | *Date* | *Comments* |
| DPO |  |  |  |
|  |
| **SIRO Sign-off (Build & Test Approval – if required)** |
| *Function* | *Officer Approving (Name)* | *Date* | *Comments* |
| SIRO |  |  |  |