Data Protection Impact Assessment

This form should be completed with a member of the Information Governance team.

Risk (Project) Owner Details

|  |  |
| --- | --- |
| Name of controller (project owner or contract signatory) |  |
| Subject/title of DPO |  |
| DPO Contact Details |  |

Step 1: Describe the Processing

When collecting or sharing personal data, the following questions need to be answered to understand how the personal data will be used.

1. Describe the Nature of Processing

|  |  |
| --- | --- |
| Question | Response (Required) |
| 1. How will you collect, use, store and delete data? | (*Will the data be stored physically or electronically? How will you receive or retrieve the data? What system will the data be kept in? How will you delete the data when it is no longer needed?)* |
| 1. What is the source of the data? | (*Does it already exist in a system, e.g. People Online? Will you be collecting it from individuals themselves via a survey? Etc*.) |
| 1. Will you be sharing data with anyone? | (*Include any other teams or business areas inside NHSPS, external stakeholders, customers, suppliers etc.)* |
| 1. You might find it useful to refer to a flow diagram or other way of describing data flows. | Add as an attachment or describe here. |
| 1. What types of processing identified as likely high risk are involved? | (*Definitions of high-risk activities can be found in* ***Appendix 1***) |

1. Describe the Scope of Processing

|  |  |
| --- | --- |
| Question | Response |
| 1. What is the nature of the data, and does it include special category or criminal offence data? | (*include data attributes such as name, contact telephone and/or email, as well as any attribute that relates to health, religion political association, race, sexuality, location or criminal data*) |
| 1. How much data will you be collecting and using? | (*How many individuals will be included? Is it just NHSPS colleagues or customers and other third parties' information too?*) |
| 1. How often? | (*Daily/weekly/monthly/annually/ad hoc*) |
| 1. How long will you keep it? | (*How long do we need the data for? Months/years? For as long as the employee is employed by NHSPS?*) |
| 1. How many individuals are affected? | (*estimate the number of individuals whose data is being used*) |
| 1. What geographical area will the data be processed in? | (*Are you collecting information to be sent overseas? Does the supplier or solution store information overseas? Where?*) |

1. Describe the Context of Processing

|  |  |
| --- | --- |
| Question | Response |
| 1. What is the nature of your relationship with the individuals (data subjects)? | (*Colleague? Customer? Another stakeholder?*) |
| 1. How much control will they have? |  |
| 1. Would they expect you to use their data in this way? |  |
| 1. Do they include children or other vulnerable groups? | (*In reference to the data collection will you identify disabilities/race or ethnicity/sexuality?*) |
| 1. Are there prior concerns over this type of processing or security flaws? |  |
| 1. Is it novel in any way? What is the current state of technology in this area? | (Is there a solution that is similar to the one you’ve proposed? If the proposed solution has never been trialled or tested previously, indicate this here.) |
| 1. Are there any current issues of public concern that you should factor in? | (*Any recent breaches via this type of system or supplier?*) |
| 1. Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |  |

1. Describe the Purpose(s) of Processing

|  |  |
| --- | --- |
| Question | Response |
| 1. what do you want to achieve? |  |
| 1. What is the intended effect on individuals? |  |
| 1. What are the benefits of the processing for the team/project/NHSPS? |  |

Step 2: Consultation Process

Consider how you will consult relevant stakeholders

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

|  |  |
| --- | --- |
| Question | Response |
| 1. Who else do you need to involve within your organisation? |  |
| 1. Do you need to ask your processors to assist? | *(Is there anything specific we need the Processer to sign up to, e.g. Cyber Essentials)* |
| 1. Do you plan to consult information security experts, or any other experts? |  |

Step 3: Assess the Necessity and Proportionality

Consider whether the data being collected is necessary and relevant

Describe compliance and proportionality measures, in particular:

|  |  |
| --- | --- |
| Question | Response |
| 1. what is your lawful basis for processing? | *(Please see the Data Protection Policy for further information on legal basis, e.g. we will obtain the consent of the data subjects)* |
| 1. Does the processing achieve your purpose? | *(Respond yes / no and provide additional information.)* |
| 1. Is there another way to achieve the same outcome? | *(Respond yes / no and provide additional information if possible, e.g. yes, but the cost of this is not feasible).* |
| 1. How will you prevent function creep? | *What controls can you implement to ensure no additional data is captured or used in a way that it shouldn’t be)* |
| 1. How will you ensure data quality and data minimisation? | *(What controls will be put in place to record any changes to data or ensure this is held accurately)* |
| 1. What information will you give individuals? | (*Do we need to draft a separate Privacy Notice or provide additional information on how their information will be used?* |
| 1. How will you help to support their rights? |  |
| 1. What measures do you take to ensure processors comply? | (*What monitoring of processes practices will be done, e.g. right to audit clause).* |
| 1. How do you safeguard any international transfers? |  |

Step 4: Identify and Assess Risks

Information risks may be related to either GDPR or more generally to the Business

Information risks can be anything from loss of data, breaching the agreed use of the data or having data accuracy issues.

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|  | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |
|  |  |  |  |

Step 5: Identify Measures to Reduce Risk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 4** | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
|  |  | Eliminated reduced accepted | Low medium high | Yes/no |
|  |  |  |  |  |

Step 6: Sign-off and Outcome

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/position/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 going ahead |
| 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: | | | |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | | |
| This DPIA will kept under review by: |  | The DPO should also review ongoing compliance with DPIA |

Appendix 1 – Types of Processing requiring DPIA

|  |  |  |
| --- | --- | --- |
| **Type of processing operation(s) requiring a DPIA** | **Description** | **Non-exhaustive examples of existing areas of application** |
| **Innovative technology** | Processing involving the use of new technologies, or the novel application of existing technologies (including AI).  A DPIA is required for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions) when combined with any other criterion from WP248rev01. | * Artificial intelligence, machine learning and deep learning * Connected and autonomous vehicles * Intelligent transport systems * Smart technologies   (including wearables) * Market research involving neuro-measurement (i.e. emotional response analysis and brain activity) * Some IoT applications, depending on the specific circumstances of the processing |
| **Denial of service** | Decisions about an individual’s access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special- category data. | * Credit checks * Mortgage or insurance applications * Other pre-check processes related to contracts (i.e. smartphones) |
| **Large-scale profiling** | Any profiling of individuals on a large scale | * Data processed by Smart Meters or IoT applications * Hardware/software offering fitness/lifestyle monitoring * Social-media networks * Application of AI to existing process |
| **Biometric data** | Any processing of biometric data for the purpose of uniquely identifying an individual.  A DPIA is required for any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion from WP248rev01 | * Facial recognition systems * Workplace access systems/identity verification * Access control/identity verification for hardware/applications (including voice recognition/fingerprint/facial recognition) |
| **Genetic data** | Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.  A DPIA is required for any intended processing operation(s) involving genetic data when combined with any other criterion from WP248rev01 | * Medical diagnosis * DNA testing * Medical research |
| **Data matching** | Combining, comparing or matching personal data obtained from multiple sources | * Fraud prevention * Direct marketing * Monitoring personal use/uptake of statutory services or benefits * Federated identity assurance services |
| **Invisible processing** | Processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort (as provided by Article 14.5(b).  A DPIA is required for any intended processing operation(s) involving where the controller is relying on Article 14.5(b) when combined with any other criterion from WP248rev01 | * List brokering * Direct marketing * Online tracking by third parties * Online advertising * Data aggregation/data aggregation platforms * Re-use of publicly available data |
| **Tracking** | Processing which involves tracking an individual’s geolocation or behaviour, including but not limited to the online environment.  A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from WP248rev01 | * Social networks, software applications * Hardware/software offering fitness/lifestyle/health monitoring * IoT devices, applications and platforms * Online advertising * Web and cross-device tracking * Data aggregation / data aggregation platforms * Eye tracking * Data processing at the workplace * Data processing in the context of home and remote working * Processing location data of employees * Loyalty schemes * Tracing services (tele-matching, tele-appending) * Wealth profiling – identification of high net-worth individuals for the purposes of direct marketing |
| **Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services** | The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children. | * Connected toys * Social networks |
| **Risk of physical harm** | Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals. | * Whistleblowing/complaint procedures * Social care records |