Data Protection Impact Checklist

Identifying the need for a DPIA

Purpose

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.

You must complete a DPIA for processing that is likely to result in a **high risk** to individuals. This includes some specified types of processing, seen at the end of this form.

It is also good practice to do a DPIA for any other major project or new supplier contract which requires the processing of personal data.

**Please refer to the DPIA policy for further information.**

Project Planning and Data Usage

|  |  |
| --- | --- |
| **Project and Data Questions** | **Response** |
| What are the aims of the project or process change? | (*Outline the purpose, benefits and milestones of the Project, referring as necessary to project proposals and other documentation you may have that is relevant to data usage*) |
| What types of data will be collected, stored, shared or analysed? | (*E.g. Contact details, location information, employee details, health information etc.)* |
| Will the data be used in any of the activities listed in **Appendix 1**? | (Yes/No) |

Recommendations

Once the above section has been completed, please email a copy of this form to [dpo@property.nhs.uk](mailto:dpo@property.nhs.uk).

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/position/date** | **Notes** |
| DPO advice provided: |  | DPO should advise on next steps for the DPIA process including: whether a full DPIA is required; whether review of DPIA is required. |
| Summary of DPO advice:   * Full DPIA required/why or why not? * Will the DPIA require a review and is an action plan required? * At which checkpoints should a review be conducted? | | |
| DPO advice accepted or overruled by: |  | If overruled, you must explain your reasons |
| Comments: | | |

**Appendix 1 – ICO High-Risk Activities**

When is a DPIA mandatory?

Below is a list of processing activities that the ICO defines as always requiring a DPIA due to the activity posing a high-risk to individuals.

|  |  |  |
| --- | --- | --- |
| 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 |