**Data Protection Impact Assessment screening checklist**

Data protection legislation makes it a legal requirement to complete a full assessment in certain cases. We also legally have to record that decision, if a project includes use of personal data. This form assesses whether a DPIA is required and captures that decision.

You need to only answer Y/N to indicate whether the criteria applies, and add notes if you are not sure or to include more details/context to justify your choice. The form includes examples from the regulator, to help understand the criteria in context.

If you need assistance whilst completing this, please contact [data-protection@qmul.ac.uk](mailto:data-protection@qmul.ac.uk)

|  |  |
| --- | --- |
| **Name of Project** |  |
| **Name of Lead** |  |
| **High level description** |  |
| ***For IG completion:***  **DPIA required** |  |

**List 1**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type of processing operation(s) requiring a DPIA** | **Description** | **Non-exhaustive examples of existing areas of application** | **Y/N** | **Notes** |
| **Systematic and extensive profiling with significant effects** | ‘systematic’ means that the processing:   * occurs according to a system; * is pre-arranged, organised or methodical; * takes place as part of a general plan for data collection; or * is carried out as part of a strategy.   The term ‘extensive’ implies that the processing also covers a large area, involves a wide range of data or affects a large number of individuals.  Significant effect: is something that has a noticeable impact on an individual and can significantly affect their circumstances, behaviour or choices. |  |  |  |
| **Large scale use of sensitive data** | The GDPR does not contain a definition of large-scale processing, but to decide whether processing is on a large scale you should consider:   * the number of individuals concerned; * the volume of data; * the variety of data; * the duration of the processing; and * the geographical extent of the processing. | * a hospital (but not an individual doctor) processing patient data; * a fast-food chain tracking real-time location of its customers; * a search engine processing data for behavioural advertising; or * individual professionals processing patient or client data are not processing on a large scale. |  |  |
| **Public monitoring** |  | CCTV |  |  |
| **Innovative technology** | Processing involving the use of new technologies, or the novel application of existing technologies (including AI). | * 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 |  | If Y, do any criteria from List 2 apply? |
| **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. | * Facial recognition systems * Workplace access systems/identity verification * Access control/identity verification for hardware/applications (including voice recognition/fingerprint/facial recognition) |  | If Y, do any criteria from List 2 apply? |
| **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. | * Medical diagnosis * DNA testing * Medical research |  | If Y, do any criteria from List 2 apply? |
| **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 informing the individual would prove impossible or involve disproportionate effort. | * List brokering * Direct marketing * Online tracking by third parties * Online advertising * Data aggregation * Re-use of publicly available data |  | If Y, do any criteria from List 2 apply? |
| **Tracking** | Processing which involves tracking an individual’s geolocation or behaviour, including but not limited to the online environment. | * 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 |  | If Y, do any criteria from List 2 apply? |
| **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 |  |  |

**List 2**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type of processing operation(s) requiring a DPIA** | **Description** | **Non-exhaustive examples of existing areas of application** | **Y/N** | **Notes** |
| **Evaluation or scoring** | Including profiling and predicting especially work performance, health, reliability or behaviour, location or movements. | * Screening customers against credit reference database * Using genetic data to predict disease or health risks * Behavioural marketing profiles |  |  |
| **Automated decision-making with legal or similar significant effect** | Taking decisions with legal effects on the person. |  |  |  |
| **Sensitive data or data of a highly personal nature** | Including special category and criminal offence data. |  |  |  |
| **Data processed on a large scale** | See points to consider for large scale in previous section. |  |  |  |
| **Data concerning vulnerable data subjects** | This is because of the increased power imbalance meaning individuals might not be able to oppose processing of their data. | * Children * employees * vulnerable segments of the population (mentally ill people, asylum seekers, elderly, patients) |  |  |

This list also includes ‘innovative use of technology’, ‘matching data’ and ‘denial of service’ and ‘public monitoring’ which are also listed on List 1.

Please send this completed form back to [data-protection@qmul.ac.uk](mailto:data-protection@qmul.ac.uk) and the team will come back to you with the next steps.

Acknowledgements: with thanks to the Barts Health IG Team.