1. High risk processing operations

Under section 35 of the Data Protection Act (DPA), controllers and processors must consult the Data Protection Office for processing operations likely to present high risks to individuals.

To determine whether processing operations are likely to present high risks, a list of criteria can be considered for evaluation taking into account the guidance of the Article 29 Working Party[1]. The list of criteria is non-exhaustive and is subject to further updates in the future, if required.

2. Criteria to consider for assessing processing operations

1) **Evaluation or scoring personal aspects/behaviour of people including profiling[2]**

> Example: The gathering of information on social networking sites by a controller to generate profiles of people.

2) **Automated decision-making producing legal or similar significant effects**

> Examples:
>
> - The setting up of a risk intelligence database by an organisation to assess individuals' credit worthiness by recording data derived from sources available to the general public, records of court proceedings and insolvency data. The organisation uses a scoring algorithm to score the individuals with respect to their credit worthiness. The risk scores are used when accepting or rejecting customers' credit applications.
> - An organisation which performs an automated selection of candidates for job interviews based on forecasted productivity.
> - The use of automated algorithms to process ethnic data which produces discriminatory / stigmatisation effects.

[1] Article 29 Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 October 2017.

[2] "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

3) Systematic monitoring by observing, monitoring or controlling data subjects

Examples:

- The systematic monitoring of individuals' online buying history and behaviour for targeted advertising.
- The use of a CCTV system to capture cars' license plates and matching them with the national database to monitor the driving conduct of individuals in a certain geographical area.

4) Sensitive data (special categories of personal data[3]) or data of a highly personal nature

Data of ''highly personal nature'' may relate to data regarding the household and private activities of an individual or data whose violation will cause serious harm such as fraud to an individual.

Example: A clinic processing physical health data and genetic data of its patients.

5) Data processed on a large scale

The term ''large scale'' may be interpreted in terms of the number of people involved, quantity/capacity of data, duration of processing or geographical area, amongst others.

Example: A public body implementing an information system for processing payment of utility bills.

[3] "special categories of personal data", in relation to a data subject, means personal data pertaining to –

(a) his racial or ethnic origin;

(b) his political opinion or adherence;

(c) his religious or philosophical beliefs;

(d) his membership of a trade union;

(e) his physical or mental health or condition;

(f) his sexual orientation, practices or preferences;

(g) his genetic data or biometric data uniquely identifying him;

(h) the commission or alleged commission of an offence by him;

(i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or

(j) such other personal data as the Commissioner may determine to be sensitive personal data.

6) **Matching or combining data sets**

Matching data sets may occur, for instance, where personal data collected for one or more purposes are compared with personal data collected for any other purpose.

> Example: Organisation A (a website) collects data of its registered users and web pages visited. Organisation B (a marketing company) has a database of customers.
>
> Organisation B uses the database of organisation A and performs a matching exercise with its database to target specific customers for marketing based on the nature of web pages visited.

7) **Data on vulnerable persons to whom the data relates (e.g. people with mental illness, asylum seekers or elderly people, patients, children, etc.)**

> Example: The implementation of an information system for an asylum.

8) **Innovative use or application of new technological or organisational solutions**

> Examples:
>
> - A system involving neuro-measurement that evaluates and monitors the physical, mental, and social effects experienced by adults and children living with neurological conditions.
> - Using Artificial Intelligence (AI) based systems

9) **When the processing "prevents data subjects from exercising a right or using a service or a contract"**

> Example: An organisation which refuses an individual's access to a service by screening its customers against a risk database.

3. Methodology to determine if a processing operation is high risk

In accordance with the Article 29 Working Party, the rule of thumb to determine whether a processing operation is likely to present high risks is that if the processing operation meets 2 or more criteria described in section 2 above, then it can be considered as likely to present high risks.

Furthermore, once a processing operation has been identified as high risk, then in accordance with section 34(1) of the DPA, controllers or processors must carry out a Data Protection Impact Assessment (DPIA) prior to the processing.

Example 1:

An intelligent video analysis system that recognise car number plates and matches them with the national database to monitor the driving behaviour in the city

Possible relevant criteria:

1) Innovative use or application of new technological or organisational solutions
2) Data processed on a large scale
3) Systematic monitoring by observing, monitoring or controlling data subjects

Since the processing meets 3 criteria, it is considered as high risk. It is therefore necessary to carry out a DPIA.

Example 2:

An editorial magazine which uses its mailing list to send daily newspapers to its subscribers

Possible relevant criteria:

1) Data processed on a large scale

Since the processing meets only 1 criterion, it is considered as low risk. It is therefore not necessary to carry out a DPIA.

In cases where it is unclear or where a processing operation meets only one criteria but the controller considers that it is high risk, it is then recommended to perform a DPIA.

At the same time, it is also important to note that even if a processing operation is not likely to present high risks, this does not in any case reduce the controller's or processor's obligation to implement appropriate security measures to protect the rights and freedoms of individuals.