Data Protection Impact Assessment Screening Guidance Notes

For section 1 (questions 1 to 12), if you answer yes to any of the questions then a Data Protection Impact Assessment (DPIA) must be carried out.

For section 2 (Additional higher risk processing activities), if you answer yes to any of the questions then you must consider whether a DPIA should be carried out. This means assessing how risky the data processing is, and whether the risks which are present should be formally considered through the DPIA process.

These guidance notes explain in more detail what the terms used in the checklist mean, and gives examples to relate these to a University context. If you are unsure whether your proposed processing falls within one of these categories, please contact the Information Governance team at dataprotection@york.ac.uk for assistance.

# Systematic and extensive profiling, automated decision-making.

## Will you use systematic and extensive profiling or automated decision-making to make significant decisions about people?

Profiling analyses aspects of an individual’s personality, behaviour, interests and habits to make predictions or decisions about them.

Automated decision-making is making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data. Automated decision-making often involves profiling, but it does not have to.

Examples of this include:

an online decision to award a loan; or

an aptitude test used for recruitment which uses pre-programmed algorithms and criteria.

A significant decision about a person is one which could have legal affects upon them, or which could noticeably affect their circumstances, behaviour or choices. It might affect their financial status, health, reputation, access to services or other economic or social opportunities.

A DPIA is required in all cases where systematic and extensive profiling or automated decision-making will be used to make significant decisions about people.

# Special category and criminal offence data

## Will you process special category data or criminal offence data on a large scale?

Special category data is personal data which reveals:

racial or ethnic origin;

political opinions;

religious or philosophical beliefs;

trade union-membership;

data concerning health;

sex life and sexual orientation;

genetic data; or

biometric data.

Criminal offence data is personal data which reveals information about actual or alleged criminal offences.

Large scale monitoring would cover:

a large geographic area;

a wide range of data;

a large volume of data;

a large number of individuals; or

a long time period of processing.

A DPIA is required in all cases where large scale processing of special category or criminal offence data will take place.

# Systematic monitoring

## Will you systematically monitor a publicly accessible place on a large scale?

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.

Large scale monitoring would cover:

a large geographic area;

a wide range of data;

a large volume of data;

a large number of individuals; or

a long time period of processing.

A DPIA is required in all cases where a publicly accessible place will be systematically monitored on a large scale.

# New Technologies

## Will you use new technologies?

New technologies means any new/cutting edge kind of technology, or novel application of existing technologies, in particular artificial intelligence.

It also includes any cloud-hosted IT system that will process personal data, special category data or criminal offence data.

This might include elements such as:

artificial intelligence, machine learning and deep learning

connected or autonomous vehicles

intelligent transport systems

smart/wearable technology

market research involving neuro-measurement (e.g. emotional response analysis and brain activity measurement)

Some Internet of Things applications

A DPIA is required in all cases where new technologies will be used.

# Access to services, opportunities and benefits

## Will you use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit?

Profiling analyses aspects of an individual’s personality, behaviour, interests and habits to make predictions or decisions about them.

In particular, this is when data is used to analyse or predict aspects of the person such as:

performance at work;

economic situation;

health;

personal preferences;

interests;

reliability;

behaviour; or

location or movements.

Automated decision-making is the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data.

Examples of this include:

an online decision to award a loan; or

an aptitude test used for recruitment which uses pre-programmed algorithms and criteria.

Automated decision-making often involves profiling, but it does not have to.

Special category data is personal data which reveals:

racial or ethnic origin;

political opinions;

religious or philosophical beliefs;

trade union-membership;

data concerning health;

sex life and sexual orientation;

genetic data; or

biometric data.

Making decisions about access to services/opportunities/benefits means decisions that are likely to have a significant or legal impact upon individuals. Examples include:

credit checks

mortgage or insurance applications

Other pre-check processes related to contracts

A DPIA is required in all cases where profiling, automated decision-making or special category data is used to help make decisions about access to services, opportunities or benefits.

# Large scale profiling

## Will you carry out profiling on a large scale?

Profiling analyses aspects of an individual’s personality, behaviour, interests and habits to make predictions or decisions about them.

In particular, this is when data is used to analyse or predict aspects of the person such as:

performance at work;

economic situation;

health;

personal preferences;

interests;

reliability;

behaviour; or

location or movements.

Large scale could mean:

large volume of data (not just wide variety)

processing over a long period of time

processing over a wide geographic extent

large number of individuals

individuals who make up a large proportion of a population (a group of individuals who have something in common)

very extensive profiling of a large number of aspects of (even a small number of) individuals.

Examples of large scale profiling are:

data processed by smart meters and/or Internet of Things applications

hardware or software offering fitness/ lifestyle monitoring

Social media networks

Application of AI to existing processes

A DPIA is required in all cases where profiling will be carried out on a large scale.

# Biometric and genetic data

## Will you process biometric or genetic data?

Biometric data means data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a person, which allow or confirm the unique identification of that person.

Examples of physical or physiological biometric identification techniques:

facial recognition;

fingerprint verification;

iris scanning;

retinal analysis;

voice recognition; and

ear shape recognition.

Examples of behavioural biometric identification techniques:

keystroke analysis;

handwritten signature analysis;

gait analysis; and

gaze analysis (eye tracking)

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a person, which give unique information about the physiology or the health of that person. Genetic data is obtained by analysis of a biological sample from the person.

Genetic data includes

medical diagnosis via genetics

DNA testing

medical research involving genetics

A DPIA is required in all cases where biometric or genetic data will be processed.

# Combining data

## Will you combine, compare or match data from multiple sources?

Combining, comparing or matching data from multiple sources refers to data coming from multiple existing repositories being used in a new way, especially to measure something about the subject.

Examples are:

fraud prevention

direct marketing

monitoring personal use or uptake of statutory services or benefits

research combining and comparing information from multiple datasets (e.g. individual schools and National Pupil Database)

federated identity assurance services

A DPIA is required in all cases where data will be combined, compared or matched from multiple sources.

# Processing without directly providing a privacy notice

## Will you process personal data without providing a privacy notice directly to the individual?

A privacy notice is a document which explains what data you will process, how and why. In most circumstances this must be provided to data subjects at the time you collect their data (sometimes shortly afterwards).

In some cases, it may be considered that providing a privacy notice to individuals would be impossible or involve disproportionate effort, and therefore processing without providing a privacy notice could be intended.

These might include:

list brokering

direct marketing

online tracking by third parties

online advertising

data aggregation/data aggregation platforms

reuse of publicly available data

A DPIA is required if personal data will be processed without providing a privacy notice directly to the individual.

# Tracking of location or behaviour

## Will you process personal data in a way which involves tracking individuals’ online or offline location or behaviour?

This means processing which involves tracking an individual's geolocation, or behaviour, including but not limited to the online environment.

Examples include:

Social networks, software applications

Hardware/software offering fitness/lifestyle/health monitoring

Internet of Things 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

A DPIA is required in all cases where personal data will be used to track individuals' online or offline location or behaviour.

# Children's data

## Will you process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?

A child is anyone under the age of 18.

Profiling analyses aspects of an individual’s personality, behaviour, interests and habits to make predictions or decisions about them.

In particular, this is when data is used to analyse or predict aspects of the person such as:

performance at work;

economic situation;

health;

personal preferences;

interests;

reliability;

behaviour; or

location or movements.

Automated decision-making is the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data.

Examples of this include:

an online decision to award a loan; or

an aptitude test used for recruitment which uses pre-programmed algorithms and criteria.

Automated decision-making often involves profiling, but it does not have to.

Marketing purposes means any purpose aimed at promoting a product or service.

Online services means websites, apps, search engines, online marketplaces and online content services such as on-demand music, gaming and video services and downloads.

A DPIA is required in all cases where children's personal data will be processed for profiling, automated decision-making, marketing purposes or to offer online services directly to them.

# Risk of physical harm

## Will you process personal data which could result in a risk of physical harm in the event of a security breach?

This is processing which is of such a kind where a personal data breach could jeopardise the [physical] health or safety of individuals.

Examples include

Whistleblowing or complaint procedures

Social care records

A DPIA is required in all cases where personal data which could result in a risk of physical harm in the event of a security breach is processed.

# Additional higher risk processing activities

The types of processing in the list below do not individually mandate that a DPIA be carried out. However, if any of these types of processing will take place, then the risks of the processing need to be considered and a DPIA undertaken if you feel that there are associated risks which should be formally considered through the DPIA process.