



Automated Decision Making and Profiling Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel are required to adhere.

Procedure Statement

This procedure sets out how North Yorkshire Police (NYP) complies with the requirements of the EU and UK General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA18) in respect of rights related to automated decision making and profiling.

Automated decision making and profiling occurs when there is any form of automated processing of personal data without human involvement. The UK GDPR gives people the right not to be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect on them.

This has strong links to the Artificial Intelligence and Machine Learning Procedure, and consideration must be given to both prior to any implementation of such systems.

Overarching Policies:

Data Protection Policy

Information Security Policy

Procedures:

DPIA Procedure

Data Procedure

Records Management Procedure

Collection and Recording of Police Information Procedure

Subject Access Procedure

Rectification and Erasure Procedure

Freedom of Information Procedure

Other Documents:

APP – Data Protection

Data Protection Consent Guidance

EDPB Guidelines on Automated Individual Decision Making and Profiling

ICO Guidelines on Big Data, Artificial Intelligence, Machine Learning and Data Protection

Process

Profiling

Article 4(4) of UK GDPR defines profiling as ‘any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.’

In general, profiling is used to find something out about individual preferences, predict their behaviour or make decisions about them. Through this collation of information, profiling creates a new set of personal data about a person.

North Yorkshire Police will carry out profiling in the following circumstances:

- If we identify associations to build links between different behaviours and attributes
- If we create profiles about people, that we then apply to them and use this to predict their behaviour
- If we collect and analyse personal data on a large scale, **using algorithms, Artificial Intelligence or machine learning**

Automated Decision Making

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 about a person.

Automated decision making can involve profiling, but it does not have to.

Benefits and Risks of Profiling and Automated Decision Making

Processing data in these ways can bring benefits to an organisation. For example, when making decisions based on large data sets, automated decision making can lead to quicker decisions and output. In a police setting, it can aid interactions with members of the public to ensure they get help quicker.

However, there are risks involved with this processing:

- Individuals may not expect their information to be used in this way, or understand how it works
- It is invisible
- The decisions can lead to adverse effects on individuals that can be significant

Right to not be subjected to solely automated decisions

Article 22(1) of the UK GDPR states that:

“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her”

This means that an individual has the right to not be subject to any of the potential processes of automated decision making or profiling. However, this right does not apply in the following circumstances:

- If the decision is authorised by law
- It is necessary for entering into or the performance of a contract
- It is based on the individual’s **explicit** consent

For special category data, a further layer is applied in Article 22(4). This states that **you can only carry out the processing if one of the above exceptions applies, and:**

- You have the individual’s explicit consent
- The processing is necessary for reasons of substantial public interest, as laid out in Schedule 1 Part 2 of the Data Protection Act 2018.

Solely automated decision making and legal or similarly significant effects

This means that the processing is totally automated, with no human involvement in the outcome. This includes where a human inputs the data into an automated system but has no influence on the outcome.

If a human interacts with the data at the end of the process, this would not be considered solely automated processing. This has to be active involvement where a human has to have the ability and discretion to alter a decision made by automated means if needed.

A legal effect on an individual is something that affects a person’s legal status or their legal rights. Equally, a decision that has similarly significant effects is something that has an equivalent impact on an individual’s circumstances, behaviours or choices. It can be unclear if an action has significant effects on an individual, however consideration of the impact of the processing and decision making on the individual’s employment, reputation, finances, employment, health, choices or behaviour should be taken into account.

The right to object to profiling

Article 21 of the UK GDPR states that individuals shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning him or her which is based on two grounds:

1. Performance of a task carried out in the public interest or legitimate interests – in this case, the organisation must stop processing this personal data unless it can show it has compelling reasons to continue the profiling that overrides the individual's interests
2. Direct marketing – processing must stop and there are no exemptions to refuse this request.

Responses to individuals exercising this right must be responded to within 1 month with confirmation of the actions taken.

Informing Data Subjects of their Rights

North Yorkshire Police must inform individuals if we are using their data for solely automated decision making where this has a legal or similarly significant effect on them.

The UK GDPR states we must provide information on:

'the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.'

This applies to direct or indirect collection of the data processed. The organisation must provide meaningful information about the logic involved and what the consequences could be for the individual.

North Yorkshire Police have a public and internal privacy notice that provides information to data subjects on this right to not be subject to this processing. This includes the process to follow to complaint and the right to complain to the Information Commissioners Office.

The data subject also has the right to access details about automated decision making. Article 15 states that the organisation must tell individuals about:

'the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.'

In this case, the Subject Access Procedure details how the organisation must respond to requests for access to personal data within the applicable time frame

Process for engaging with automated decision making and profiling

The Data Protection team **must** be consulted prior to the processing of any personal data through automated means in order to ensure the rights and freedoms of the data subject are upheld.

The DPIA procedure must be followed at all times by all NYP personnel when engaging with new automated processing and profiling techniques in all situations.

Following the DPIA procedure will also allow the risks to individuals to be considered and procedures put in place to mitigate those risks in line with the organisations data protection obligations. It also allows consideration of implementation of quality checks, removal of bias from systems, ensures special category data is considered on its own merit and **encourages auditing of machine learning tools to check for rationales and consistency.**

In line with the DPA18 principles, NYP also have an obligation to ensure that the data we use is accurate. The process included in this policy also allows consideration and implementation of key quality checks on the data being input into AI and Machine Learning to ensure that data integrity and quality is maintained to the highest standards throughout the information lifecycle.

Upon receiving a DPIA screening form, the Data Protection team will assess the request under UK GDPR and DPA18 to ensure there are adequate considerations and protections for personal data (including special category information) and issue further guidance and requirements to the business area. Information Security will also issue advice and guidance on meeting the requirements of the organisation under the Information Security Policy.

Any unauthorised use of AI or Machine Learning should be reported to the Compliance Team as soon as possible to be investigated for potential personal data breaches, under the Security Incident Reporting procedure.

Responsibilities

All NYP personnel - To note the content of this document and related policies and procedures and take personal responsibility for the security of NYP information. To engage with the data protection team in the implementation of automated processing and profiling techniques.

First Line Supervision - To ensure their team members comply with and note the content of related policies and procedures and take personal responsibility for the security of NYP information.

Information Asset Owner - To ensure their team members note and comply with the content of related policies and procedures and take personal responsibility for the security of NYP information. To act as the decision maker/assurer and ensure appropriate governance and resources are in place to effectively manage any identified risks associated with automated processing and profiling. To maintain and update the Information Asset Register when required to account for this processing.

Senior Information Risk Owner (SIRO) - responsibility for ensuring appropriate technical and/or organisational measures for personal data are implemented, together with any risks to information and the business.