GUIDELINES ON AUTOMATED DECISION-MAKING AND PROFILING FOR THE PURPOSES OF THE GDPR

Profiling and automated decision-making (ADM) are used in an increasing number of sectors. Whereas it can increase efficiency and save resources these processes can pose significant risks for individuals' rights.
In 2018, the EDPB issued guidelines on automated individual decision-making and profiling for the purposes of the GDPR. This briefing summarises the main ideas of these guidelines.

PROFILING

Profiling implies gathering data about a person and evaluating their characteristics or behavioural patterns to place them into a certain category to analyse and/or make predictions (art. 4(4) GDPR)
Profiling is composed of three elements:
- It has to be an automated form of processing
- It has to be carried out on personal data, and
- Its objective must be to evaluate personal aspects of an individual: analysing or making predictions about a person

It involves a series of statistical deductions and it comprises three stages:
- Data collection
- Automated analysis to identify correlations
- Applying the correlation to an individual to identify characteristics of present or future behaviour

PROFILING BASED ON LEGITIMATE INTERESTS

When relying on legitimate interests to creates profiles, the controller must carry out a balancing exercise to assess whether their interests are overridden by the data subject's interests or rights. Of particular relevance are:
- The level of detail of the profile
- The comprehensiveness or the profile
- The impact of the profiling
- The safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling

It may be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes (tracking across multiple websites, locations, devices, etc)

PROFILING THAT INVOLVES SPECIAL CATEGORIES OF DATA

Profiling can create special categories of data by inference from data which is not special category data in its own right but becomes so when combined with other data (e.g. state of health from food shopping).
If sensitive preferences or characteristics are inferred from profiling, the controller should make sure that:
- The processing is not incompatible with the original purpose
- They have identified a lawful basis for processing sensitive data
- They inform the data subject accordingly

AUTOMATED DECISION-MAKING

Solely automated decision-making is the ability to make decisions by technological means without human involvement. These decisions can relate to:

- Data directly provided by the individual (registration information)
- Data observed about the individual (e.g. location data)
- Data derived or inferred (such as a profile)

PROFILING AND AUTOMATED DECISION MAKING IN THE GDPR

In the context of the GDPR, profiling can be used as :

- General profiling
- Decision-making based on profiling; and
- Solely automated decision-making, including profiling, that produces legal or significantly similar effects on the data subject (art. 22 GDPR)

SPECIFIC PROVISIONS ON SOLELY AUTOMATED DECISION-MAKING

Art. 22(1) GDPR provides that

- As a rule, there is a general prohibition on fully automated individual decision-making, including profiling, that has a legal or similarly significant effect;
- There are exceptions to this rule;
- Where one exception applies, there must be measures in place to safeguard the data subject's rights

DECISIONS BASED ON SOLELY AUTOMATED PROCESSING

Art. 22(1) refers to decisions where there is no human involvement in the decision process.
For human involvement, controllers must ensure that any oversight of the decision is meaningful, rather than a token gesture, and carried out by somebody who has the authority and the competence to change the decision.

LEGAL OR SIMILARLY SIGNIFICANT EFFECTS

'*Legal effects*' requires that the decision affects somebody's legal rights or status.
A decision '*similarly significantly affects him or her*' if it produces an effect that is equivalent or similarly significant in its impact, even if there is no change in their legal rights or status. The effects of the processing must be sufficiently great or important to be worthy of attention and must have the potential to:

- Significantly affect the circumstances, behaviour or choices of the individuals concerned;
- Have a prolonged or permanent impact on the data subject; or
- Lead to the exclusion or discrimination of individuals

In many typical cases, the decision to present **targeted advertising** will not have a similarly significant effect on individuals. However, it is possible it may do, depending on the circumstances, including:

- The intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
- The expectations and wishes of the individuals;
- The way the advert is delivered, or
- Using knowledge of the vulnerabilities of the data subject

Processing having little impact on certain individuals may have a significant impact on vulnerable groups

Qubit Privacy

EXCEPTIONS FROM THE PROHIBITION
While in principle taking automated decisions that have legal or similarly significant effects are forbidden, there are some exceptions to this rule in art. 22(2) GDPR
- Performance of a contract. Controllers must show that the processing is necessary, considering less intrusive methods.
- Authorised by EU or member state law,
- Explicit consent from the data subject

SPECIAL CATEGORIES OF PERSONAL DATA
Automated decision-making that involves special categories of data (art. 22(4) GDPR) are only allowed if
- There is an applicable art. 22(2) GDPR exception; and
- Processing is based only on explicit consent (art. 9(2)(a) GDPR) or is necessary for substantial public interest based on EU or national law (art. 9(2)(g) GDPR)

CHILDREN AND PROFILING
Since children represent the most vulnerable group of society, organisations should refrain from profiling children for marketing purposes (recital 38 and 70)

RIGHTS OF THE DATA SUBJECTS
Controllers must provide specific, easily accessible information about ADM (arts. 13(2)(f), 14 (2)(g) and 15(1)(h) GDPR). In particular, they must
- Tell the individuals they are engaging in ADM
- Provide meaningful information about the logic involved.
  - The logic involved is the rationale behind or the criteria relied on in reaching the decision. While it is not required a complex explanation of the algorithm, the information must be sufficiently comprehensive for the data subject to understand the reasons for the decision.
- Explain the significance and envisaged consequences of the processing.
  - Information must be provided about intended or future processing, and how the ADM might affect the data subject. Understandable and real examples should be given, along with visual techniques.

By exercising the right to access individuals can become aware of a decision made concerning him or her. The controller must provide them with general information (e.g. factors taken into account to take the decision and their relative weight)

APPROPRIATE SAFEGUARDS

Controllers must implement appropriate measures to safeguard data subjects' rights (art. 22(3) GDPR)

At least, controllers must ensure to data subjects:

- Human intervention in the decision: somebody who has the appropriate authority and capability to change the decision
- Express their point of view
- Contest the decision

While recital 70 allows data subjects to obtain an explanation of the decision reached after the assessment, this provision is not included in the GDPR articles. However, the only way to contest a decision, which is guaranteed by art. 22(3) GDPR, is to fully understand the decision and on what basis it was made.

Controllers must also introduce appropriate procedures and measures to prevent errors, inaccuracies or discrimination on the basis of special categories of data.

- Data Protection Impact assessment
  - A DPIA must be undertaken where the controller carries out a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning them or similarly significantly affects them (art. 35(3)(a) GDPR). This provision refers to evaluations including profiling and decisions that are based on automated processing, even if they are not solely based on automated processing.
- Appoint a data protection officer
  - A DPO must be appointed where the profiling and/or the ADM is a core activity of the controller and requires regular and systematic monitoring of data subject on large scale (art. 37(1)(b) GDPR