BRODIES LLP

GDPR - AUTOMATED DECISION MAKING AND PROFILING

The General Data Protection Regulation introduces specific controls in relation to certain kinds of automated decision making and profiling. This guide provides an overview of what is changing and how the GDPR will be interpreted by supervisory authorities, such as the UK's Information Commissioner (ICO).

What is automated decision making and profiling?

Automated decision making and profiling are two separate, but often interlinked concepts.

Profiling is a form of automated processing of personal data used to analyse or predict matters relating to an individual. For example analysing an individual's performance at work, financial status, health, interests or location.

Automated decision making is the ability to make decisions without human involvement. In practice, profiling can often be a precursor to automated decision making.

Profiling and automated decision making can be used in three ways:

General profiling	Decision making based on profiling	*Solely* automated decision making
Individuals are segmented into different groups based on data analysis	A human makes a decision based on profiling	An alogrithm makes a decision with no human input

General prohibition on certain types of automated decision making

The Article 29 Working Party's draft guidance interprets Article 22(1) of the GDPR as prohibiting decisions based solely on automated decision making which produce legal effects or similarly significantly affect an individual unless:

- It is necessary for the performance of or entering into a contract;
- It is authorised by law; or
- It is based on the data subject's explicit consent.

Automated decision making that involves special categories of personal data, such as information about, health, sexuality, and religious beliefs, is only permitted where it is carried out on the basis of explicit consent or where it is necessary for reasons of substantial public interest, such as fraud prevention and operating an insurance business.

Necessity is interpreted narrowly, and organisations must be able to show that it is not possible to use less intrusive means to achieve the same goal.

Further regulatory guidance on what constitutes 'explicit' consent is expected in due course. As with general consent under the GDPR, any consent must be freely given, unambiguous, specific and informed.

What is meant by 'legal effects' or 'similarly significantly affects'?

'Legal effects' are things that have an impact on an individual's legal rights or affect a person's legal status or rights under a contract. Examples include:

- Being entitled or denied benefits such as housing or child benefit
- Being refused entry at a national border
- Automatic disconnection from a mobile phone service because an individual forgot to pay their bill

'Similarly significantly affects' means decisions that have non-trivial consequences, such as:

- Automatic refusal of an online credit application
- Automated decisions about credit limits, based on analysis of spending habits and location

Can I get round the restrictions on by having a human supervise the decision?

No. Any human intervention must be meaningful. The individual must analyse all available data and have the authority and competence to change the decision.

What do I need to tell individuals?

Where decisions are made solely using automated decision making, organisations must:

- tell the individual that it is using automated decision making for these purposes;
- provide meaningful information about the logic involved (for example by explaining the data sources and main characteristics of the decision making process); and
- explain the significance and envisaged consequences

The Article 29 Working Party recommends that these steps are followed whenever automated decision making is used, as this can help with ensuring that the processing is carried out fairly.

Safeguards and transparency

Individuals must be told when a decision has been taken solely using automated decision making and they must have the right to request a review of the decision. The review should be .by a person with appropriate authority and capacity to change the decision and should involve a thorough review of all relevant information.

Organisations using automated decision making should also carry our regular reviews and use appropriate procedures to prevent errors.

Data Protection Impact Assessment

When considering using automated decision making and profiling, organisations should assess the risks using a data protection impact assessment. Conducting a DPIA will help organisations show that appropriate measures have been put in place to mitigate those risks and help demonstrate compliance with the GDPR.

Organisations should also remember that any use of automated decision making and profiling must comply with the general principles in the GDPR in relation to fair and lawful processing. Processing will also be subject to the general rights of individuals under the GDPR, including the right to object to certain types of processing (including direct marketing), the right of rectification and the right to erasure.

Find out more

The Article 29 Working Party's draft guidance on profiling can be downloaded from its website.

Key contacts

To discuss how the GDPR will impact on your organisation, or how Brodies can assist you with your preparations, please get in touch with a member of Brodies' data protection and information law team.

Grant Campbell
PARTNER
+44 (0)131 656 0115
grant.campbell@brodies.com

Martin Sloan
PARTNER
+44 (0)131 656 0132
martin.sloan@brodies.com

More information

You can follow the latest developments on the GDPR, including the latest guidance from regulators, on our GDPR microsite:
brodies.com/GDPR
or our blog:
http://techblog.brodies.com