UK ICO Publishes Discussion Paper on Profiling and Automated Decision-Making under GDPR

APRIL 13, 2017

The UK Information Commissioner's Office (ICO) continues to play an active role in shaping data protection law in the EU, notwithstanding the UK's decision to leave the EU in the aftermath of Brexit. On April 6, 2017, the ICO issued a discussion paper containing its "initial thoughts" on profiling and automated decision-making under the General Data Protection Regulation (GDPR). The deadline for submitting comments is April 28, 2017.

As profiling continues to increase in importance and scope for many businesses, companies may look to the ICO's discussion paper as an early indication of its views and concerns on key profiling issues. In addition, companies may want to submit comments to the ICO to address specific profiling issues raised by their businesses and to influence how the GDPR is ultimately interpreted and implemented in practice.

The ICO's discussion paper is part of its continuing efforts to help businesses prepare for the GDPR, which takes effect on May 25, 2018. For example, the ICO recently finished accepting comments on its draft guidance on the meaning of "consent" under the GDPR, and it intends to publish additional guidance in the future.

Discussion Paper on Profiling and Automated Decision-Making Under the GDPR

The GDPR introduced several new rights and obligations with respect to "profiling" and automated decision-making. The ICO's discussion paper highlights some of the key areas of profiling that the ICO felt needed further consideration. Although the ICO states that its discussion paper "should not be interpreted as guidance," the ICO indicates that it is taking a leading role on this issue as part of the Article 29 Working Party (the collective group of EU data protection authorities that is charged with issuing guidance on EU privacy laws). The Article 29 Working Party's guidelines on profiling are due to be published later this year.

Definition and Scope of Profiling

The ICO appears to view the definition and scope of profiling—and the corresponding rights and obligations that go with it—broadly. Article 4(4) of the GDPR defines profiling as "[a]ny 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." The ICO states that, broadly speaking, it considers profiling to mean "gathering information about an individual or group of individuals and analysing their characteristics or behaviour patterns in order to place them into a certain category or group, and/or to make predictions or assessments about their: ability to perform a task; interests; or likely behaviour."

The ICO notes that the "widespread availability of personal data on the internet and advances in technology, coupled with the capabilities of big data analytics mean that profiling is becoming a much wider issue, reflected in the more detailed provisions of the GDPR." In particular, the ICO notes that the types of data used to build profiles may include, but are not limited to:

- internet search and browsing history;
- education and professional data;
- data derived from existing customer relationships;
- data collected for credit-worthiness assessments;
- financial and payment data;
- consumer complaints or queries;
- driving and location data;
- property ownership data;
- information from store cards and credit cards;
- consumer buying habits;
- wearable tech, such as fitness trackers;
- lifestyle and behavior data gathered from mobile phones;
- social network information;
- video surveillance systems;
- biometric systems;
- internet of things; and
- telematics.

Finally, the ICO solicits comments on whether there must be a predictive element, or some degree of inference for the processing to be considered profiling. In its discussion paper, the ICO appears to suggest that profiling may include an analysis of personal aspects even if there is not a predictive element or inference being drawn.

Complying With the GDPR's Key Requirements in the Profiling Context

Beyond discussing the definition and scope of profiling, the ICO's discussion paper focuses on interpreting, applying, and soliciting feedback on many of the GDPR's key requirements in the profiling context. For example, the ICO notes that companies must have a legal basis to engage in profiling, but suggests that consent may be difficult to obtain in the profiling context because consent must be freely given, specific, informed, and unambiguous. Similarly, if the data controller takes the position that profiling is necessary for the purpose of the performance of a contract or for the legitimate interests of the controller or third party, the ICO indicates that the company must be

able to demonstrate that the profiling is "necessary" to achieve that purpose, rather than simply "useful."

The ICO's discussion paper also offers suggestions on complying with many of the GDPR's other requirements, such as those related to transparency; data minimization, accuracy, and retention; lawful processing; rectification and objection to profiling; implementation of appropriate safeguards; and children's data.

GDPR Requirements That are Unique to Profiling

The ICO also provides suggestions and solicits comments on issues that are unique to profiling under the GDPR. For example, the ICO considers the circumstances under which decisions based on profiling may qualify as producing a "legal" or "significant" effect, since such decisions are subject to specific rules under the GDPR. The ICO notes that a "**legal**" effect might be something that "adversely impacts an individual's legal rights, or affects their legal status" and that a "**significant**" effect "suggests some consequence that is more than trivial and potentially has an unfavourable outcome." The ICO provides specific examples of such potential effects—for example, those that cause individuals to change their behavior in a significant way—but notes that it "may be useful to establish an external recognised standard to measure such effects, instead of simply relying upon the subjective view of the controller or the data subject."

Importantly, the ICO suggests that a wide range of activities may qualify as involving a "**systematic and extensive evaluation of personal aspects** relating to natural persons which is based on automated processing, including profiling, and on which decisions are based **that produce legal effects** concerning the natural person **or similarly significantly affect the natural person**" (emphasis added) and therefore would require a "data protection impact assessment" under Article 35(3)(a). *According to the ICO, such activities may include*:

- profiling and scoring for purposes of risk assessment (for example for credit scoring, insurance premium setting, fraud prevention, detection of money laundering);
- location tracking, for example by mobile apps, to decide whether to send push notifications;
- loyalty programs;
- behavioral advertising; and
- monitoring of wellness, fitness, and health data via wearable devices.

It is worth noting that a recent draft opinion by the Article 29 Working Party on data protection impact assessments under the GDPR also endorses a similarly broad view of the scope and requirements of Article 35(3)(a).

Finally, the ICO's discussion paper highlights the GDPR's requirement that companies must provide individuals with a right to object to profiling in certain contexts and requests feedback on what companies may consider to be a "compelling legitimate grounds" for profiling that overrides the "interests, rights, and freedoms" of the individual.

Authors

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207